

VŠB – Technická univerzita Ostrava  
Fakulta elektrotechniky a informatiky  
Katedra informatiky

**Analýza transakcí v platební síti  
Bitcoin pomocí komplexních sítí  
Analysis of the Bitcoin Payment  
Transactions Using Complex  
Networks**

# Zadání diplomové práce

Student:

**Bc. Jan Tyc**

Studijní program:

N2647 Informační a komunikační technologie

Studijní obor:

1801T064 Informační a komunikační bezpečnost

Téma:

**Analýza transakcí v platební síti Bitcoin pomocí komplexních sítí**  
**Analysis of the Bitcoin Payment Transactions Using Complex Networks**

Jazyk vypracování:

čeština

Zásady pro vypracování:

Diplomová práce se zabývá analýzou transakcí v internetové platební síti Bitcoin pomocí komplexních sítí. Úkolem studenta bude modelovat dynamiku transakcí v této platební síti pomocí komplexních sítí a tyto sítě následně analyzovat.

Pokyny pro vypracování:

1. Seznamte se s problematikou internetové platební sítě Bitcoin
2. Nastudujte způsoby modelování dynamických systémů pomocí komplexních sítí. Zaměřte se zejména na sítě sociální a temporální
3. Nastudujte odborné publikace, které popisují analýzu sítě Bitcoin. Poznatky shrňte v textové části práce popisující tzv. state-of-the-art
4. Navrhněte způsob modelování dynamik platební sítě Bitcoin pomocí komplexních sítí
5. Shromážděte data a proveďte jejich analýzu. Nezapomeňte při tom na statistiku
6. Z analýzy vyvoďte závěr a vše podrobně zpracujte do textové části práce.

Seznam doporučené odborné literatury:

- [1] NAKAMOTO, Satoshi, et al. Bitcoin: A peer-to-peer electronic cash system. 2008.
- [2] DECKER, Christian; WATTENHOFER, Roger. Information propagation in the bitcoin network. In: IEEE P2P 2013 Proceedings. IEEE, 2013. p. 1-10.
- [3] RON, Dorit; SHAMIR, Adi. Quantitative analysis of the full bitcoin transaction graph. In: International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013. p. 6-24.
- [4] SCHOLTES, Ingo, et al. Causality-driven slow-down and speed-up of diffusion in non-Markovian temporal networks. Nature communications, 2014, 5: 5024.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Lenka Skanderová, Ph.D.**

Datum zadání: 01.09.2019

Datum odevzdání: 30.04.2020



  
doc. Ing. Jan Platoš, Ph.D.  
vedoucí katedry

  
prof. Ing. Pavel Brandštetter, CSc.  
děkan fakulty

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 15. května 2020

.....  
Týp Jan

Souhlasím se zveřejněním této diplomové práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v magisterských programech VŠB-TU Ostrava.

V Ostravě 15. května 2020

.....  
Tyl Jan

Rád bych na tomto místě poděkoval všem, kteří mi s prací pomohli, protože bez nich by tato práce nevznikla. Rád bych poděkoval mé vedoucí práce za trpělivost a dobré rady.

## **Abstrakt**

Tato práce se zabývá analýzou transakcí Bitcoinu pomocí komplexních sítí. Cílem této práce je převod transakcí do podoby komplexních a temporálních sítí a analyzovat vlastnosti, které by mohly indikovat výrazný nárůst či pokles ceny Bitcoinu nebo případnou manipulaci ceny.

Bitcoin je kryptoměnou, která v době psaní této práce opět získává na popularitě po svém pádu v roce 2017. Důkazem toho je i fakt, že se lidé snaží protlačit Bitcoin na Wall Street. Mnoho odborníků tvrdí, že obecně kryptoměny mají před sebou skvělou budoucnost a nahradí tak tradiční finanční prostředky.

**Klíčová slova:** Bitcoin, blockchain, komplexní sítě, temporální sítě, analýza

## **Abstract**

This thesis is focused on Bitcoin transaction analysis with the help of complex and temporal networks. The goal of this thesis is converting Bitcoin transactions into the form of complex and temporal networks and analyze properties, that could indicate significant increase or decrease in the Bitcoin price or eventual manipulation of Bitcoin price.

Bitcoin is a cryptocurrency, which is at the time of writing this thesis, again gaining popularity despite its fall in 2017. The evidence for that is a fact, that people are trying to get Bitcoin to the Wall Street. Many experts say, that cryptocurrencies generally have a great lookout for the future and eventually replace the traditional financial resources.

**Keywords:** Bitcoin, blockchain, complex networks, temporal networks, analysis

# Obsah

<b>Seznam použitých zkratk a symbolů</b>	<b>9</b>
<b>Seznam obrázků</b>	<b>10</b>
<b>Seznam tabulek</b>	<b>11</b>
<b>1 Úvod</b>	<b>12</b>
<b>2 Aktuální výzkum</b>	<b>13</b>
<b>3 Princip fungování kryptoměny Bitcoin</b>	<b>17</b>
3.1 Základní rysy Bitcoinu a blockchain . . . . .	17
3.2 Princip fungování transakcí v Bitcoinu . . . . .	17
3.3 Princip těžby Bitcoinu . . . . .	18
<b>4 Komplexní sítě a jejich vlastnosti</b>	<b>19</b>
4.1 Graf . . . . .	19
4.2 Komplexní síť . . . . .	23
<b>5 Experimentální část</b>	<b>24</b>
5.1 Příprava a plánování analýzy . . . . .	24
5.2 Statická analýza . . . . .	26
5.3 Dynamická analýza . . . . .	45
5.4 Analýza adres . . . . .	51
5.5 Analýza výskytu velkých pohybů . . . . .	56
<b>6 Pokračování analýzy</b>	<b>58</b>
<b>7 Závěr</b>	<b>59</b>
<b>Literatura</b>	<b>60</b>
<b>Přílohy</b>	<b>62</b>
<b>A Velké obrázky a tabulky</b>	<b>63</b>



## Seznam použitých zkratk a symbolů

SPV	– Simplified Payment Verification
MF-DFA	– Multi-Fractal Detrend Fluctuation Analysis
VPN	– Virtual Private Network
Tor	– The Onion Router

## Seznam obrázků

1	Graf viditelnosti a horizontální graf viditelnosti . . . . .	14
2	Příklad pseudo-spam transakce [7] . . . . .	15
3	Motýlková struktura Bitcoinové sítě [8] . . . . .	15
4	Rozdíl mezi silně a slabě souvislým grafem . . . . .	20
5	Ilustrace sestrojení grafu z dat . . . . .	25
6	Příklad identifikace velkého pohybu na svíčkovém grafu . . . . .	26
7	Příklady distribucí stupňů . . . . .	34
8	Průběh průměrného stupně uzlů u velkých pohybu. . . . .	47
9	Průběh průměrného stupně uzlů u malých pohybu. . . . .	48
10	Distribuce stupně v jednotlivých časových oknech u velkých pohybu. . . . .	48
11	Distribuce stupně v jednotlivých časových oknech u malých pohybu. . . . .	49
12	Distribuce vstupního a výstupního stupně u velkých pohybu. . . . .	49
13	Distribuce vstupního a výstupního stupně u malých pohybu. . . . .	50
14	Distribuce betweenness u velkých pohybu. . . . .	50
15	Distribuce betweenness u malých pohybu. . . . .	50
16	Distribuce excentricity u velkých pohybu. . . . .	51
17	Distribuce excentricity u malých pohybu. . . . .	51
18	Zastoupení identifikovaných unikátních adres u velkých pohybu. . . . .	55
19	Zastoupení identifikovaných unikátních adres u malých pohybu. . . . .	55
20	Distribuce stupně v jednotlivých časových oknech u velkých pohybu. . . . .	64
21	Distribuce stupně v jednotlivých časových oknech u malých pohybu. . . . .	64
22	Distribuce vstupního a výstupního stupně u velkých pohybu. . . . .	65
23	Distribuce vstupního a výstupního stupně u malých pohybu. . . . .	65
24	Distribuce betweenness u velkých pohybu. . . . .	66
25	Distribuce betweenness u malých pohybu. . . . .	66
26	Distribuce excentricity u velkých pohybu. . . . .	67
27	Distribuce excentricity u malých pohybu. . . . .	67

## Seznam tabulek

1	Tabulka velkých pohybů stažených pro analýzu . . . . .	25
2	Tabulka velkých pohybů stažených pro analýzu . . . . .	27
3	Tabulka malých pohybů stažených pro analýzu . . . . .	28
4	Tabulka počtů vrcholů a hran . . . . .	30
5	Tabulka statistických hodnot pro vrcholy a hrany . . . . .	30
6	Tabulka počtů smyček a vícenásobných hran . . . . .	31
7	Tabulka statistických hodnot pro smyčky a vícenásobné hrany . . . . .	32
8	Tabulka stupňů vrcholů . . . . .	32
9	Tabulka statistických hodnot pro stupeň vrcholů . . . . .	33
10	Tabulka průměrů sítí . . . . .	35
11	Tabulka statistických hodnot pro průměr sítě . . . . .	36
12	Tabulka délky průměrných cest . . . . .	36
13	Tabulka statistických hodnot pro průměrnou délku cesty . . . . .	37
14	Tabulka počtů silně a slabě propojených komponent . . . . .	38
15	Tabulka statistických hodnot pro počty silně a slabě propojených komponent . . . . .	38
16	Tabulka velikostí největší silně a slabě propojené komponenty . . . . .	39
17	Tabulka statistických hodnot pro velikosti největších propojených komponent . . . . .	39
18	Tabulka shlukovacích koeficientů . . . . .	40
19	Tabulka statistických hodnot pro shlukovací koeficient . . . . .	41
20	Tabulka údajů související s betweenness centralitou . . . . .	42
21	Statistika betweenness centrality (BC) a zastoupení uzlů s nulovou BC . . . . .	43
22	Tabulka stupňové asortativity . . . . .	44
23	Tabulka statistických hodnot pro stupňovou asortativitu . . . . .	44
24	Tabulka reciprocity hran . . . . .	45
25	Tabulka statistických hodnot pro stupňovou asortativitu . . . . .	46
26	Tabulka označení temporální sítě a příslušného datumu . . . . .	46
27	Tabulka unikátních adres u velkých pohybů . . . . .	53
28	Tabulka unikátních adres u malých pohybů . . . . .	53
29	Tabulka počtu velkých pohybů v závislosti na dni v týdnu . . . . .	56
30	Tabulka počtu velkých pohybů v závislosti na dni v měsíci . . . . .	57
31	Tabulka počtu vrcholů v temporálních sítích . . . . .	68
32	Pokračování tabulky počtu vrcholů v temporálních sítích . . . . .	69
33	Tabulka počtu hran v temporálních sítích . . . . .	70
34	Pokračování tabulky počtu hran v temporálních sítích . . . . .	71
35	Tabulka průměrných stupňů v temporálních sítích . . . . .	72
36	Pokračování tabulky průměrných stupňů v temporálních sítích . . . . .	73

# 1 Úvod

Cílem této práce je zjistit, jakými vlastnostmi se charakterizují sítě, které zachycují velký pohyb ceny Bitcoinu za dvě hodiny a zda jde pomocí temporálních sítí predikovat takový pohyb. Také se budu snažit najít charakteristiky, které by mohly indikovat potenciální velký pohyb v blízké budoucnosti. Motivací této práce je vytvoření postupu, který by dokázal predikovat nadcházející velký pohyb ceny Bitcoinu, případně vytvoření postupu, který by dokázal odhalit manipulaci ceny na základě několika subjektů.

Blockchain je technologie, pomocí které lze vytvořit decentralizovanou a konzistentní databázi. V dnešní době tato technologie stále nabírá na popularitě, přičemž je tato oblast aktivně zkoumána výzkumníky po celém světě. Pravděpodobně nejznámější zástupci blockchainu jsou kryptoměny v čele s nepopíratelně nejznámějším Bitcoinem. Cílem kryptoměn obecně je vytvořit alternativní finanční ekosystém, který není centrálně řízen pomocí bank a institucí, jak je tomu u tradičních finančních prostředků.

V této práci nejdříve popíšu nejaktuálnější způsoby analýzy, které už byly na Bitcoinu prováděny a shrnu jejich závěry. Poté popíšu, jak Bitcoin funguje a z čeho se skládá. Následující kapitola se bude zabývat problematikou komplexních sítí, kde nastíním zásadní koncepty, které budou v práci využívány. Další kapitola bude popisovat mnou navrženou metodiku transformace Bitcoinových transakcí do komplexní sítě a temporální sítě. Dále popíšu metody a výsledky analýzy komplexní sítě, které budou použity při analýze transakcí. V předposlední kapitole uvedu, jak by se tato analýza dala vylepšit a na závěr pak shrnu své poznatky.

## 2 Aktuální výzkum

Transakce Bitcoinu už byly několikrát analyzovány. Transakce u Bitcoinu je přesun této kryptoměny od jednoho vlastníka k jinému. Hlubší vysvětlení pojmu transakce je v kapitole 3.2.

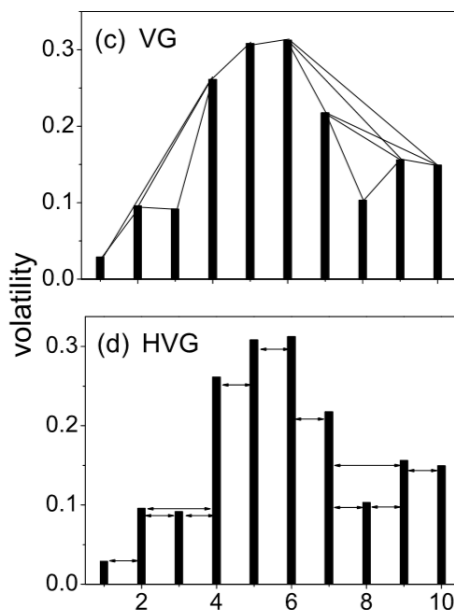
Jeden z přístupů analýzy transakcí Bitcoinu [1] vychází z denní ceny Bitcoinu a sestrojuje tzv. grafy viditelnosti a horizontální grafy viditelnosti, které jsou následně analyzovány. Princip sestrojování těchto neorientovaných grafů spočívá v tom, že se v histogramu denní ceny Bitcoinu kreslí přímkami mezi dvěma vrcholy v histogramu. Tento postup je vidět na Obrázku 1. Pokud tato příčka neprotne žádný jiný sloupec v histogramu, tak se mezi těmito dvěma uzly v grafu viditelnosti vytvoří hrana. Na podobném principu je založena tvorba horizontálního grafu viditelnosti, s tím rozdílem, že se mezi body kreslí pouze horizontální přímkami. Data, ze kterých se konstruují tyto grafy viditelnosti obsahují 1849 denních záznamů ceny Bitcoinu z dat 28.4.2013 až do 20.5.2018. Při následné analýze komunit se objevila podobnost s komunitami z analýzy slunečních skvrn pomocí komplexních sítí [2]. Porovnávána byla volatilita, což je změna hodnot mezi jednotlivými dny. V případě Bitcoinu je to změna ceny a v případě slunečních skvrn to byla změna aktivity v čase. Tato vlastnost odhaluje přítomnost významných flukтуаčních cyklů v Bitcoinu. Dále článek odhaluje přítomnost HUBů, které odpovídají událostem, které extrémně zahýbaly cenou Bitcoinu.

Analýzou Bitcoinu se také zabývá italská vědecká skupina Maesa, Marino a Ricci, která zatím vydala 4 vědecké články zabývající se analýzou Bitcoinu, které shrnu v následujících odstavcích.

Ve své první práci [3] používají data od roku 2009 až do roku 2015. Tato práce vytváří tzv. "graf uživatelů". Nejprve se adresy, které jsou na vstupech transakcí přidávají do skupin. Tyto skupiny pak mají reprezentovat jednotlivé uživatele v Bitcoinové síti. Z těchto skupin se pak vytváří orientovaný graf a to tím způsobem, že se jednotlivé skupiny převedou na uzly a pokud existuje transakce mezi adresami v jednotlivých skupinách, pak mezi nimi existuje orientovaná hrana. Tato síť měla ve výsledku přes 46 milionů uzlů a přes 294 milionů hran. Výsledkem této práce je objevení několika vlastností takto zkonstruované sítě. V této síti se objevuje fenomén "rich-get-richer", což by odpovídalo vlastnostem preferenčního připojování nových uzlů. Dále se objevila existence několika centrálních uzlů s vysokým stupněm a vysokou harmonickou centralitou, které slouží jako mosty. To jsou uzly, které spojují různé části sítě, kdy například hranami spojují dvě velké komunity. Také se zjistilo, že tato síť má větší průměr než je tomu například u sociálních sítí [4], ale i přesto se jedná o model small-world.

Článek, který navazuje na předchozí práci [5] zkoumal stejně zkonstruovanou síť z pohledu topologie a časového vývoje. Tato práce potvrdila všechny objevy z předchozí práce (rich-get-richer, existence centrálních uzlů). Z časové analýzy pak vyplynulo, že počet uzlů v síti a počet transakcí roste exponenciálně. V průběhu času také rostl výstupní stupeň uzlů, což indikuje větší počet odeslaných transakcí.

Stejná vědecká skupina pak zkoumala i výskyt nezvyklého chování transakcí [6], které vypadalo jinak, než je obvyklé u transakcí, které se jinak v Bitcoinu běžně vyskytují a vyjadřují



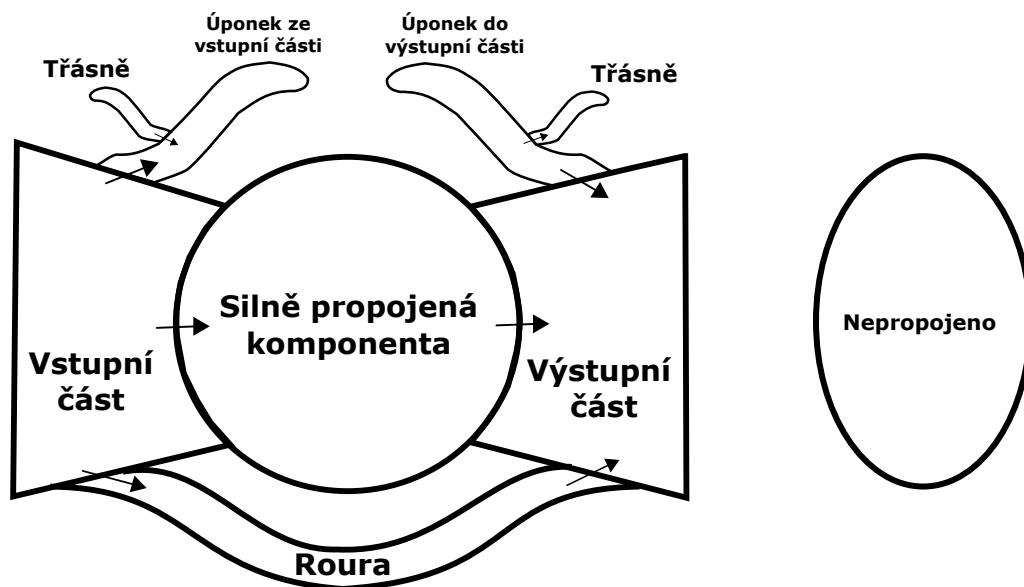
Obrázek 1: Graf viditelnosti a horizontální graf viditelnosti

legitimní přesun Bitcoinů z jednoho účtu na jiný. Analyzují hlavně distribuci vstupního stupně vrcholů, pomocí které odhalili právě tyto PS-transakce. Objevily se totiž transakce, které měly jeden vstup, a výstupů bylo v řádu desítek až stovek, přičemž hodnota transakce byla vždy 0.0001 BTC až na jednu transakci, která poslala zbytek neposlaných Bitcoinů zpět autorovi této transakce. Adresa, kam se tento zbytek poslal, pak sloužila jako zdroj další transakce stejného typu. Autoři této práce tyto transakce pak pojmenovali jako PS-transakce (pseudo-spam transakce), a celou posloupnost takovýchto transakcí pojmenovali jako pseudo-spam řetěz. Příklad takové transakce je na Obrázku 2. Tento typ transakcí vykazoval anomálii v distribuci stupňů podle vstupního stupně. Anomálie spočívala v tom, že se našly uzly s takovým vstupním stupněm, jejichž množství narušuje tvar mocninného rozdělení zbytku vstupního stupně. Autoři pak diskutují nad významem těchto transakcí. V úvahu připadají spam útoky na blockchain, či permanentní reklama uložena v blockchainu. Autoři také zkoumají vlastnosti těchto pseudo-spam řetězů z pohledu statistiky.

Zatím nejnovější článek této vědecké skupiny [8] opět vychází ze stejného uživatelského grafu, ale tentorát uzly rozděluje do různých rolí, ze kterých pak vyplývá tzv. "Motýlková struktura", která byla představena v práci [9]. Z Obrázku 3 je patrný název této struktury. Ze samotné struktury se zjistilo, že přes 86% uživatelů Bitcoinové sítě patří do silně propojené komponenty, přičemž 9% uživatelů s touto komponentou nijak neinteraguje. Další analýza ukázala, že drtivá většina výměny Bitcoinu probíhá v silně propojené komponentě, přičemž největší zůstatek mají uzly ve výstupní části, což jsou uzly, do kterých vede hrana ze silně propojené komponenty, ale ne zpět. Také bylo zjištěno, že většina těžařů patří do vstupní části, což je skupina, ze které vede hrana do silně propojené komponenty, ale už ne naopak. Pojem silně propojená komponenta je

Hash	35dead89c059e846e2013a06a70cd84a7ba0f80da7741c283d6...	2015-07-13 05:10
	13hBbRdWGLCDNkDR8Pyf6jw3wM3q4EwbTF 0.09297420 BTC	
	14CLqCNphUJ54ro2PtqQWJdmW3Eic1WmUd 0.00001000 BTC	
	1LdCb7UmFBomBjgnAsL5GGVjPx2zmgeH5j 0.00001000 BTC	
	1946NEo8LmCfCMjqWwCZUbdptrKZjstLD9 0.00001000 BTC	
	1MufD4JJZStpry94QisNaxP1qm8IESdwc 0.00001000 BTC	
	18RtMr82Nrt7TAvtan9Lr1XLngQ5dQTsm 0.00001000 BTC	
	1H6wM8Xj8GNrhqWBrnDugd8Vf3nAfZgmNq 0.00001000 BTC	
	1MBDpvDZWfWkwcehZAKtbwT3uFPBcRYMcG 0.00001000 BTC	
	1Jing1eBufhzQooZ7QYVVrehPJvPZaw6fJ 0.00001000 BTC	
	16R5FAhBg5DXxayye8nkQsPGecaYJc74cH 0.00001000 BTC	
	19DtQVEryym7Jbi2eXfTpZenJpxttsGsM3 0.00001000 BTC	
	1BFLDATk4IE6R2hyTfQnJxBZYctU9eshCM 0.00001000 BTC	
	1KApySLevseC2EYDZiwbL1tXoGe2zyNEA 0.00001000 BTC	
	1AgDYTxr9FDGa7oXbVhuHxmJJALKqs8cip 0.00001000 BTC	
	1BrufVILKnSWtuWGkryPsKsxonV2NQ7Tcj 0.00001000 BTC	
	1NrPN24makqVwvuDuhcUY2cCZQUYrjv9bB 0.00001000 BTC	
	13gWbKbeeG75MhasvG9auEZYXUWzruhRsc 0.00001000 BTC	
	16ccTEPgka5zkrfBNzN2CJviAARoFcER9a 0.00001000 BTC	
	1MHMLCSdxzyaBEYQsQYYPYkaBjeV1aSNZ 0.00001000 BTC	
	1DMXuMp2f6HeC2fLCDY6vYPghxVuW6Tuap 0.00001000 BTC	
	1GTLXA2C2ksFbyabsgaAiYMFgzv2DfNSkS 0.00001000 BTC	
	Load more outputs... (81 remaining)	
Fee	0.00071840 BTC (20.006 sat/B - 5.001 sat/WU - 3591 bytes)	0.09225580 BTC

Obrázek 2: Příklad pseudo-spam transakce [7]



Obrázek 3: Motýlková struktura Bitcoinové sítě [8]

vysvětlena v kapitole 4.1.1. Ostatní části motýlkového grafu (úponky a třásně) jsou části, které interagují se vstupní nebo výstupní částí, ale nepatří do silně propojené komponenty.

Další práce [10] se zabývala časovou analýzou bitcoinové sítě, a objevila dvě časová období Bitcoinu z dat Bitcoinu do roku 2013. První časové období Bitcoinu probíhalo do podzimu roku 2010. Jelikož to byla nová technologie, tak nebyla hojně využívána, tudíž často nastávaly velké výkyvy ve vlastnostech sítě. Poté přišlo druhé časové období, kdy se začal Bitcoin více používat a začaly ho přijímat i firmy a charakteristiky sítě se ustálily. Také autoři přišli na to, že vývoj bitcoinové sítě se řídí preferenčním připojováním, což má vliv na akumulování bohatství. Objevil se totiž vztah mezi stupněm uzlu a bohatstvím příslušného uzlu. Jedná se o další článek, kdy se opět potvrdila exponenciální distribuce vstupních a výstupních stupňů uzlů, a vývoj distribuce zůstatků jednotlivých uzlů se také řídí exponenciálním průběhem.

Zajímavá práce na kterou jsem dále narazil, se zaměřila na analýzu prvních čtyř let Bitcoinu [11]. Tato práce analyzuje jak se bitcoinová síť vyvíjela. Analýza ukázala, že většina transakcí souvisela s gamblingem, 63% všech transakcí bylo v rozmezí od 1 satoshi (1 satoshi = 0,00000001 BTC) až po 1 BTC a okolo 1,6% IP adres bylo nějakým způsobem skryto (VPN, Tor, Proxy). Analýza distribuce stupňů ukázala, že se jedná o bezškálovou síť. Největší HUBy v síti byly řízeny burzou Mt. Gox, gamblingovou službou satoshiDICE a službou webových peněženek InstaWallet. Součástí práce jsou i vizualizace sítě, které přehledněji ukazují výsledky analýzy.

V oblasti Bitcoinu se zkoumaly i vlastnosti ve spojitosti s náhodností a chaosem [12]. Zde autoři také identifikovali dvě časová období Bitcoinu podobně jako předchozí článek. Tato práce ovšem analyzovala větší časový úsek Bitcoinu a to až do data největšího dosavadního rozmachu Bitcoinu, což je druhá polovina roku 2017. Tento výzkum pracoval s metodami orientovanými na náhodnost a chaos, jako je například Shannonova entropie, či MF-DFA. Výsledkem této analýzy je, že vývoj ceny vykazuje a zahrnuje chaotické chování. Výnos Bitcoinu se značí vysokou nejistotou a to i v pozdější fázi bitcoinu. Vývoj ceny i výnos bitcoinu vykazuje multifraktalitu, což znamená, že je nelze jednoduše popsat jednou fraktální dimenzí.

Poslední článek v této sekci zkoumal síť po měsících od počátku kryptoměn až po poslední den v říjnu roku 2017 [13]. Práce se zaměřila na Bitcoin, Ethereum a Namecoin. Síť byla vytvářena ze samotných transakcí. Výzkum byl cílen na dvě části. První část se zabývala akumulovaným růstem sítě a druhá část zkoumala topologii měsíční sítě. To je temporální síť, kdy jedno časové okno popisuje jeden měsíc vývoje ceny. Autoři argumentují tím, že tento typ sítě bude lépe zachycovat dynamiku kryptoměn. Opět se zde objevují dvě časové období kryptoměn a to období počáteční a období, kdy se kryptoměna rozšíří a začíná být využívána. Analýza také ukázala, že síť transakcí kryptoměn se ne vždy musí zhušťovat, což znamená, že uzly a hrany i ubývají. Autoři také zkoumali, zda distribuce stupňů v těchto sítích následuje mocninné rozdělení, přičemž statistický test toto tvrzení zamítnul.



### 3 Princip fungování kryptoměny Bitcoin

Jelikož se v této práci zabývám analýzou transakcí Bitcoinu pomocí komplexních sítí, rozhodl jsem se zde umístit kapitolu stručně vysvětlující základní návrh a fungování kryptoměny Bitcoin, a to z důvodu lepšího pochopení následné analýzy.

#### 3.1 Základní rysy Bitcoinu a blockchain

Bitcoin vznikl v roce 2009 [14] a funguje na technologii zvané blockchain. Blockchain v případě Bitcoinu slouží jako veřejná kniha transakcí, která není kontrolována a schvalována žádnou centrální autoritou, ale je decentralizována. O schvalování a kontrolu informací do něj zapsaných se stará veřejná peer-to-peer síť nezávislých uzlů.

Základní jednotkou blockchainu je blok a ten slouží pro ukládání informací do samotného blockchainu. V případě Bitcoinu se do něj ukládají informace o proběhlých transakcích. Jedná se o data typu: kdo transakci vytvořil, komu je určena, kolik kryptoměny se v rámci této transakce pošle a mnoho dalšího. Tyto bloky jsou identifikovány unikátním identifikátorem, který je spočítán pomocí kryptografické hašovací funkce, do jejíhož vstupu jsou zahrnuty informace z jednotlivých transakcí. Podstatnou informací, kterou blok obsahuje je odkaz na předchozí blok, čímž se jednotlivé bloky spojují do dlouhého seznamu bloků se sekvenčním přístupem.

Použitím kryptografické hashovací funkce a jednosměrně zřetěženého seznamu je zajištěna konzistence dat. V případě že by se potenciální útočník snažil o pozměnění informací jedné transakce v bloku, musel by útočník změnit informace také ve všech blocích, které tento blok následují. Taková změna je sice možná, ale je výpočetně nesmírně náročná.

#### 3.2 Princip fungování transakcí v Bitcoinu

Základní jednotkou bloku v blockchainu je transakce, která nese informace o samotných přesunech Bitcoinů. V případě Bitcoinu se fyzicky neposílají žádné Bitcoin, ale pouze se mění stav peněženek jednotlivých stran, které jsou v transakci zahrnuty. Jednotlivé strany v transakci jsou chráněny svými digitálními podpisy, veřejnými klíči a otisky vypočítanými z těchto veřejných klíčů. Všechny tyto komponenty jsou součástí ověřovacího mechanismu Bitcoinu. Tímto se zajišťuje, že odesílatel může odeslat pouze Bitcoin, které byly poslány právě jemu.

Jednotlivé transakce se skládají ze vstupů a výstupů. Vstupy zde určují, odkud Bitcoin pochází a výstupy určují, kam mají Bitcoin směřovat. V rámci transakcí se tvoří něco jako řetěz transakcí, kdy každý vstup má v sobě uchování informaci o výstupu, ze kterého se Bitcoin budou posílat. Vysvětlím na zjedodušeném příkladě, kdy budu považovat, že jedna transakce bude mít právě jeden vstup a právě jeden výstup.

Řekněme, že existuje osoba, která si chce koupit mobilní telefon v prodejně, kde se dá platit Bitcoinem. Tato osoba si nejprve koupí Bitcoin například skrze službu Coinbase. Tímto se vytvoří transakce, kdy na vstupu bude adresa služby Coinbase a na výstupu bude adresa peněženky té

dané osoby. Následně při platbě v obchodě s elektronikou se vytvoří další transakce, kdy na výstupu bude peněženka obchodu s elektronikou. Na vstupu té samé transakce bude adresa peněženky kupujícího s tím, že na tom stejném vstupu bude ještě odkaz na výstup transakce, pomocí které si kupující koupil Bitcoin.

### 3.3 Princip těžby Bitcoinu

Těžbou se v případě Bitcoinu zabývají speciální uzly v síti na těžbu zaměřené. Tyto uzly se v dnešní době spojují do skupin (anglicky pool), protože jedinec nemá při dnešním výpočetním výkonu Bitcoinové sítě šanci vytěžit ani jeden blok sám. Tyto těžební uzly mají za úkol vytvářet nové bloky z poslaných transakcí. V rámci bloku je první transakce vždy takzvaná coinbase transakce, která nemá žádný vstup. Výstup této transakce vyplňují těžaři svou vlastní adresou. Pro vytvoření bloku se používá algoritmus důkazu práce (anglicky proof-of-work).

Tento algoritmus funguje tak, že se z nasbíraných nepotvrzených transakcí vytvoří blok. Součástí hlavičky každého bloku je také položka zvaná nonce. Úkolem těžaře je pak najít takovou nonci, která po spočítání otisku hlavičky bloku splňuje určitou podmínku. V případě Bitcoinu je to počet nul na začátku daného otisku. Tato podmínka se pak aktualizuje každých 2016 bloků. Mění se podle toho, kolik času zabralo vytěžit těchto 2016 bloků. Reaguje se tímto na celkový výkon sítě. Pokud se do těžby zapojí více uzlů, výpočetní čas se zkrátí a tím pádem následuje ztížení těžebních podmínek v podobě většího počtu začínajících nul v otisku bloku.

Tímto se také udržuje doba těžby jednoho bloku. V průměru by se měl vytěžit jeden blok za 10 minut. Tuto dobu ale nelze při decentralizaci uhlídat, tudíž ve skutečnosti mohou být dva po sobě následující bloky vytěženy například v rámci pěti minut.

## 4 Komplexní síť a jejich vlastnosti

### 4.1 Graf

Základním stavebním kamenem komplexních sítí jsou grafy. Jedná se o strukturu, která reprezentuje množinu objektů, u kterých následně definujeme jejich propojení mezi sebou. Teorie grafů se používá při modelování reálných situací, přičemž tato struktura zachovává informaci o topologii, ale může zanedbat informaci o přesné poloze. Rovnice 1 formálně popisuje graf [15]. Je to množina vrcholů (někdy se jim říká i uzly) a hran.

$$G = (V, E) \quad (1)$$

Podle typu hrany se pak grafy dále rozlišují. Neorientované grafy obsahují neorientované hrany (Rovnice 2) a orientované grafy pak obsahují hrany orientované (Rovnice 3) [15].

$$E \subseteq \{\{u, v\} | u, v \in V\} \quad (2)$$

$$E \subseteq V \times V \quad (3)$$

U neorientovaného grafu jsou jednotlivé hrany definovány jako neuspořádaná dvojice z množiny vrcholů. Orientovaný graf na druhou stranu zachovává i informaci o směru hrany, takže orientovaná hrana je definována jako uspořádaná dvojice z množiny vrcholů.

Pro vysvětlení vlastností grafů je potřeba si zavést pár klíčových pojmů z teorie grafů [15].

- Sled - Posloupnost vrcholů a hran, kde mezi dvěma sousedními vrcholy v posloupnosti existuje hrana
- Cesta - Sled, ve kterém se neopakují vrcholy
- Podgraf - Podgraf  $G'$  je podmnožinou grafu  $G$ , který neobsahuje všechny hrany či vrcholy z grafu  $G$ .

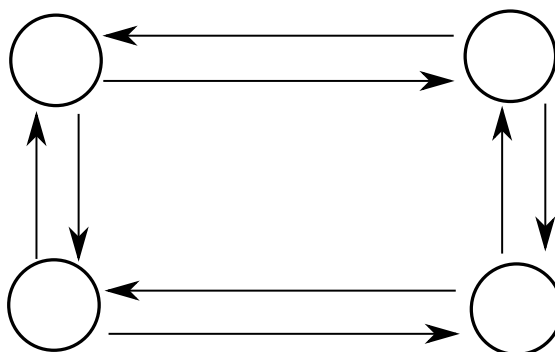
#### 4.1.1 Souvislost grafu

Souvislost grafů popisuje, zda je možné se z jakéhokoli uzlu dostat do libovolného jiného uzlu v grafu. Neorientovaný graf je souvislý právě tehdy, pokud pro každé dva vrcholy  $X$  a  $Y$  existuje sled z vrcholu  $X$  do vrcholu  $Y$ . Pokud je graf nesouvislý, jednotlivé podgrafy, které nejsou mezi sebou propojeny se nazývají komponenty souvislosti.

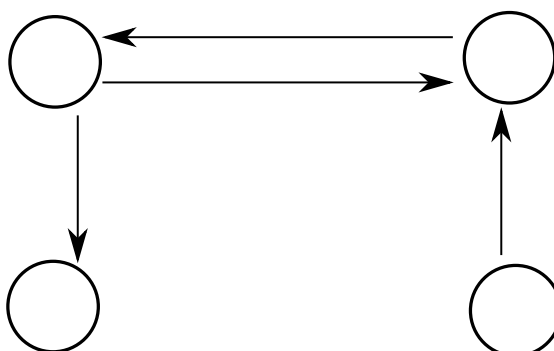
U orientovaných grafů se pak souvislost dělí na dva druhy [16]. Znázornění rozdílu mezi silnou a slabou souvislostí je na Obrázku 4.

- Silná souvislost - Graf je silně souvislý, pokud pro každé dva vrcholy  $X$  a  $Y$  existuje cesta z  $X$  do  $Y$  i cesta z  $Y$  do  $X$ .

### Silně souvislý graf



### Slabě souvislý graf



Obrázek 4: Rozdíl mezi silně a slabě souvislým grafem

- Slabá souvislost - Graf je slabě souvislý, pokud existuje cesta mezi všemi dvojicemi vrcholů, pokud zanedbáme orientaci hran.

#### 4.1.2 Hustota grafu

Hustota grafu vyjadřuje jak blízko je graf k úplnému grafu (graf, kde existuje hrana mezi všemi dvojicemi vrcholů). Pokud je tedy výsledek hustoty například 0,5, znamená to, že graf obsahuje polovinu ze všech možných hran.

Vzorec výpočtu hustoty pro neorientovaný graf je zapsán v Rovnici 4. Verze pro orientovaný graf je pak vidět z Rovnice 5. Jediným rozdílem mezi těmito dvěma výpočty je ten, že u neori-

entovaných grafů se každá hrana do výpočtu zahrne dvakrát [17]. Proměnné  $E$  resp.  $V$  vyjadřují množiny hran resp. množiny vrcholů.

$$D = \frac{2|E|}{|V| \cdot (|V| - 1)} \quad (4)$$

$$D = \frac{|E|}{|V| \cdot (|V| - 1)} \quad (5)$$

#### 4.1.3 Stupeň vrcholu

Stupeň vrcholu znázorňuje kolik vrcholů je incidentní s daným vrcholem. Jinak řečeno kolik vrcholů je s daným vrcholem spojeno hranou. Formálně zapsaný výpočet stupně vrcholu pro neorientovaný graf je v Rovnici 6 [15]. Uzlům s vysokým stupněm se také často říká HUBy. Proměnné  $u$  a  $v$  ve vzorcích níže vyjadřují vrcholy.

$$\deg(v) = |\{u : \{v, u\} \in E\}| \quad (6)$$

U orientovaných grafů se výpočet dělí na vstupní stupeň resp. výstupní stupeň. Vzorce pro výpočet jsou v Rovnici 7 resp. Rovnici 8.

$$\deg^+(v) = |\{u : (u, v) \in E\}| \quad (7)$$

$$\deg^-(v) = |\{u : (v, u) \in E\}| \quad (8)$$

U vstupního stupně vrcholu se jedná o to, kolik hran do vrcholu  $V$  vstupuje a naopak u výstupního vrcholu se jedná o počet vrcholů, které z vrcholu  $V$  vychází.

#### 4.1.4 Nejkratší cesta, průměr a excentricita

Hledání nejkratších cest v grafu je problém, který se prolíná mnoho oblastmi (umělá inteligence ve hrách, navigace, optimalizace, směřování v počítačových sítích apod.). V případě mé sítě je nejkratší cesta v grafu dána nejmenším počtem přeskoků mezi dvěma uzly. Existuje však i varianta pro vážené sítě, kdy je každá hrana ohodnocena nějakou metrikou (délka cesty v kilometrech, kapacita přenosového kanálu apod.). V tomto případě se pak hledá taková cesta, která vede přes takové hrany, které mají ve výsledku nejnižší součet dané metriky. Pro výpočet nejkratších cest se používá Dijkstraův algoritmus nebo  $A^*$  algoritmus.

Další vlastností, která se týká nejkratších cest je průměr sítě. Tato hodnota odpovídá nejdelší nejkratší cestě v síti.

Excentricita je vlastnost, kterou jsem počítal u temporálních sítí. Tato vlastnost vrcholu v grafu vyjadřuje nejvzdálenější vrchol od daného vrcholu. Maximální excentricita grafu pak odpovídá průměru grafu.

#### 4.1.5 Shlukovací koeficient

Shlukovací koeficient vyjadřuje, do jaké míry jsou sousední uzly daného uzlu propojeny mezi sebou. Jinak řečeno kolik hran z maximálně možných se v sousedství vyskytuje [18].

Abychom byli schopni zavést formální definici pro shlukovací koeficient, je nutno nejprve zavést pojem sousedství. Sousedství vrcholu  $V$  je množina vrcholů, které jsou s vrcholem  $V$  napřímo spojeny hranou.

Toto sousedství se pak bere v potaz při počítání lokálního shlukovacího koeficientu. Ten je definován jako podíl mezi existujícími vrcholy mezi uzly v sousedství a maximálním možným počtem hran, který se v daném sousedství může vyskytovat.

Následně se z těchto lokálních shlukovacích koeficientů počítá globální shlukovací koeficient. Jedná se o průměr shlukovacích koeficientů spočítaný přes všechny vrcholy v síti [18].

Matematické vyjádření lokálního shlukovacího koeficientu pro neorientovaný resp. orientovaný graf je v Rovnici 9 resp. Rovnici 10 [19]. Proměnná  $E_i$  popisuje počet hran spojující sousední vrcholy daného vrcholu, pro který je počítán lokální shlukovací koeficient. Proměnná  $K_i$  vyjadřuje stupeň vrcholu, pro který je počítán shlukovací koeficient.

$$C_i = \frac{2E_i}{|K_i| \cdot (|K_i| - 1)} \quad (9)$$

$$C_i = \frac{E_i}{|K_i| \cdot (|K_i| - 1)} \quad (10)$$

Po spočítání lokálního shlukovacího koeficientu, pak lze spočítat průměrný shlukovací koeficient pro celou síť podle Rovnice 11, kdy  $N$  je počet všech vrcholů v síti.

$$\overline{C} = \frac{1}{N} \sum_{i=1}^N C_i \quad (11)$$

#### 4.1.6 Betweenness centralita

Když se v teorii grafu řekne pojem centralita, jedná se o vlastnost, která popisuje důležitost uzlu v grafu. V tomto případě betweenness centralita přiřazuje každému uzlu důležitost na základě nejkratších cest. Čím více nejkratších cest uzlem v grafu prochází, tím vyšší má betweenness centralitu. Vzorec pro výpočet betweenness centrality je v Rovnici 12 [20]. Ve vzorci pak  $\sigma_{st}$  odpovídá celkovému počtu nejkratších cest mezi uzly  $s$  a  $t$  a  $\sigma_{st(v)}$  je počet nejkratších cest mezi uzly  $s$  a  $t$ , které vedou přes vrchol  $v$ .

$$B = \sum_{s \neq t \neq v} \frac{\sigma_{st(v)}}{\sigma_{st}} \quad (12)$$

#### 4.1.7 Reciprocita hran

Reciprocita hran je vlastnost, která se dá spočítat pouze u orientovaných grafů. Tato charakteristika vyjadřuje podíl hran, které spojují dva vrcholy a vedou obousměrně. Formální zápis je pak vidět v Rovnici 13 [21], kdy proměnná  $R$  popisuje počet hran, které jsou opětovány a proměnná  $U$  je počet neopětovaných hran.

$$r = \frac{R}{R + U} \quad (13)$$

#### 4.1.8 Stupňová asortativita

Poslední vlastností kterou zde uvedu, je stupňová asortativita. Jedná se v podstatě o Pearsonův korelační koeficient a vyjadřuje, do jaké míry se uzly se stejným stupněm spojují hranami. Hodnota asortativity se pohybuje v intervalu  $< -1, 1 >$ , přičemž hodnota blízko 1 znamená, že jsou uzly spojeny s uzly se stejným stupněm, hodnota blízko -1 indikuje spojení vrcholů s vrcholy, které mají výrazně jinou velikost stupně a hodnota okolo nuly neukazuje žádnou korelaci spojování uzlů v závislosti na stupni vrcholu. Vzorec je vidět v Rovnici 14 [22]. Proměnná  $e_{xy}$  vyjadřuje podíl hran, které spojují vrcholy  $x$  a  $y$ , proměnné  $a_x$  resp.  $b_y$  jsou podíly hran, které začínají a končí ve vrcholu  $x$  resp. ve vrcholu  $y$ . Proměnné  $\sigma_a$  resp.  $\sigma_b$  jsou směrodatné odchylky distribucí  $a_x$  resp.  $b_y$ .

$$r = \frac{\sum_{xy} xy (e_{xy} - a_x b_y)}{\sigma_a \sigma_b} \quad (14)$$

## 4.2 Komplexní síť

Komplexní sítě jsou grafy, které obsahují netriviální topologické vlastnosti. Grafy s triviálními vlastnostmi jsou například mřížky nebo kompletní grafy. Komplexní sítě jsou výsledkem výzkumu reálných vztahů mezi subjekty.

Komplexní sítě se dělí do čtyř základních skupin [23].

- Sociální - hrany představují sociální vztahy
- Informační - vrcholy reprezentují informace, hrany (odkazy) spojují informace (např. citační síť)
- Technologické - sítě pro distribuci komodit (např. silniční síť)
- Biologické - sítě aplikovatelné na biologický systém (např. neuronové sítě)

## 5 Experimentální část

V této kapitole nejprve zjistím, jakými vlastnostmi se charakterizují statické sítě, které zachycují velký pohyb ceny Bitcoinu za dvě hodiny a následně se pokusím pomocí temporálních sítí predikovat velký pohyb. Také se budu snažit najít charakteristiky, které by mohly indikovat potenciální velký pohyb v blízké budoucnosti. Cílem je vytvoření postupu, který by dokázal predikovat nadcházející velký pohyb ceny Bitcoinu, případně vytvoření postupu, který by dokázal odhalit manipulaci ceny na základě několika subjektů.

V této části představím výsledky mé analýzy. Při analýze jsem používal nástroje Gephi a Pajek. Pro stahování dat a pro konverzi dat do formátu komplexní sítě jsem použil své řešení v programovacím jazyku Python. Některé analýzy byly také provedeny v jazyce Python s pomocí knihovny Networkx. Pro část analýzy dynamiky komplexních sítí jsem použil také jazyk R.

### 5.1 Příprava a plánování analýzy

Po seznámení se s existujícími analýzami transakcí kryptoměny Bitcoin za pomocí komplexních sítí jsem objevil dva nejčastější způsoby analýzy. Jeden ze způsobů, typičtější pro práce, které zkoumaly transakce v rané době Bitcoinu, analyzoval čisté transakce, tak jak jsou zapsány v Bitcoinu. To znamená, že uzly v následných komplexních sítích jsou identifikovány svou adresou. Druhý způsob analýzy sdružoval adresy do subjektů. Sdružování probíhalo tak, že se všechny adresy objevující se na jednom vstupu přiřadily k jednomu subjektu. Pokud se tedy některá adresa vyskytovala na vstupu u dvou různých transakcí, jednalo se ve výsledné síti o ten stejný uzel (subjekt).

V mé práci jsem se rozhodl použít přístup analýzy samotných transakcí. Důvodem je fakt, že sdružování transakcí nemusí být stoprocentní. Může nastávat situace, kdy si jeden subjekt pro každou transakci vygeneruje novou adresu a posílá transakce, které mají na vstupu pouze jednu adresu. Jedna z dalších situací, která může nastat, je, že se na vstupu transakce objeví adresy patřící stejnému subjektu, ale tyto adresy se vyskytnou u právě jedné transakce a nepřekryjí se se vstupy s jinými transakcemi patřící stejnému subjektu.

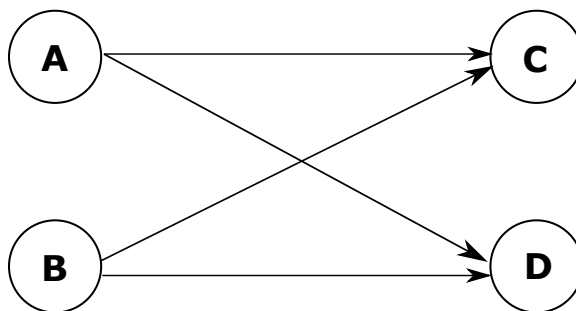
Z tohoto přístupu vyplývá, že jsem se rozhodl použít orientované sítě, které zachycují toky transakcí. Orientovaná hrana mezi uzly A a B existuje právě tehdy, pokud je na vstupu transakce adresa A, a na výstupu transakce adresa B. Pokud se jedná o transakce s jednou adresou na vstupu a více adresami na výstupu, existují hrany mezi adresou na vstupu a všemi adresami na výstupu. Toto platí i pro případ, kdy je více adres na vstupu s tím, že je každá adresa na vstupu spojena orientovanou hranou se všemi adresami na výstupu. Tento způsob sestrojení grafu ilustruje Obrázek 5 a Tabulka 1.

Dále jsem musel najít vhodný zdroj dat pro analýzu transakcí. Mojí první volbou bylo použití veřejného API, které poskytují data ohledně Bitcoinu. Tyto nástroje často poskytují informace, které nejsou v samotném blockchainu, ale dají se z celého blockchainu extrahovat. Příklad takových informací je: seznam všech transakcí dané adresy, možnost obousměrného procházení



Vstupy	Hodnota (BTC)	Výstupy	Hodnota (BTC)
A	2	C	3
B	2	D	1

Tabulka 1: Tabulka velkých pohybů stažených pro analýzu



Obrázek 5: Ilustrace sestrojení grafu z dat

blockchainu, nebo zjištění, zda je výstup přeposlán dál, či nikoliv. Takové možnosti práce s Bitcoinem poskytují velký prostor pro následnou analýzu těchto dat. Avšak po určitém čase používání těchto nástrojů se objevily podstatné vady. Jednou z vad byla nestabilita takových prostředků, kdy se stávalo, že API bylo po velkou část dne nedostupné a tím pádem se přerušilo stahování dat, a poté nebylo možno navázat tam, kde se stahování přerušilo. Druhým velkým problémem byla rychlost stahování dat. API které jsem vyzkoušel byly [24] a [25].

Druhou možností jak sehnat data transakcí, bylo nainstalování bitcoinového klienta, nechat ho stáhnout celý blockchain, který má v době psaní práce okolo 300 GB a následně stahovat data z něj. Tím se vyřešily oba problémy a hlavně problémy s rychlostí, jelikož počítač na kterém byl bitcoinový klient nainstalován měl SSD disk a optické připojení k Internetu.

V dalším kroku následoval výběr dat. Zde jsem postupoval následovně. Otevřel jsem si svíčkový graf ceny Bitcoinu (co je to svíčkový graf lze vidět na Obrázku 6) a hledal jsem největší pohyby za rok 2019. Velký pohyb jsem si definoval tím, že za danou hodinu proběhl pokles nebo růst ceny minimálně o 300 dolarů. Když jsem takový pohyb našel, podíval jsem se poté přesně o týden zpátky, kde jsem téměř vždy našel pohyb několikanásobně menší. Na Obrázku 6 je ilustrace takového pohybu. Daný pohyb odpovídá 2. dubnu 2019 v čase 04:00 UTC. Tato svíčka v grafu se formuje od 03:00 až do 04:00 UTC. Mým plánem bylo zachytit celou dobu formování svíčky a k tomu ještě půl hodiny před touto svíčkou a půl hodiny po této svíčce. Tomu odpovídá časové období od 02:30 UTC až do 04:30 UTC.

Tímto mi vznikly dvě sady sítí. Jedna sada dat zachycovala sítě odpovídající velkému pohybu a druhá sada dat zachycovala sítě znázorňující malý pohyb ceny Bitcoinu. Celkem jsem takto získal 20 sítí s velkým pohybem a 20 sítí s malým pohybem, které byly použity pro statickou analýzu sítí. Tyto informace jsou zachyceny v Tabulce 2 resp. v Tabulce 3. Tabulky popisují



Obrázek 6: Příklad identifikace velkého pohybu na svíčkovém grafu

informace o velkých resp. malých pohybech. Časy jednotlivých bloků jsem se snažil co nejvíce přiblížit hodnotám časů, které jsem si určil.

Pro dynamickou analýzu sítě jsem poté vybral 10 největších pohybů z těchto dvaceti. V tomto případě jsem nestahoval bloky v rámci určitého časového období, ale stáhl jsem 20 bloků, začínající půl hodiny po ukončení formování velké svíčky. Důvodem byl fakt, že jsem potřeboval stejný počet časových oken do následných temporálních sítí. V Tabulkách 2 a 3 jsou tyto případy označeny symbolem '\*’.

Při tvorbě temporálních sítí jsem postupoval následovně. Oproti transakcím v agregované síti pro statickou analýzu měly transakce pro temporální síť navíc ještě identifikátor 0 až 19 podle toho, z jakého bloku pochází. Na základě těchto identifikátorů se pak vytvořila temporální síť s 20 časovými okny s odpovídajícími transakcemi.

## 5.2 Statická analýza

Prvním krokem analýzy byla analýza vlastností a charakteristik statické sítě. Důvodem této analýzy byla snaha zjistit výrazné rozdíly ve vlastnostech sítí s velkým a malým pohybem. Pokud by se takový výrazný rozdíl podařilo najít, mohlo by se jednat o vlastnost, podle které by se dalo určit, zda nastane velký pohyb v ceně Bitcoinu či nikoliv.

V následujících tabulkách budou jednotlivé řádky identifikovány pouze datem velkého pohybu. Dále pro přehlednost budou buňky s vyšší hodnotou označeny tučným písmem. Pro každou

	Poslední blok (UTC)	První blok (UTC)	Počet bloků	Rozdíl ceny
26.10.2019 1:00 *	26.10.2019 01:34	25.10.2019 23:27	9	1140 \$
24.09.2019 18:00 *	24.09.2019 18:30	24.09.2019 16:30	15	870 \$
06.08.2019 10:00 *	06.08.2019 10:29	06.08.2019 08:32	15	650 \$
26.06.2019 20:00 *	26.06.2019 20:30	26.06.2019 18:29	21	2000 \$
27.06.2019 16:00 *	27.06.2019 16:38	27.06.2019 14:30	16	830 \$
18.12.2019 22:00	18.12.2019 22:37	18.12.2019 20:23	17	319 \$
04.12.2019 13:00	04.12.2019 13:28	04.12.2019 11:33	13	560 \$
25.11.2019 12:00	25.11.2019 13:05	25.11.2019 10:11	10	350 \$
22.11.2019 10:00	22.11.2019 10:36	22.11.2019 08:25	16	480 \$
25.10.2019 15:00 *	25.10.2019 15:27	26.10.2019 13:27	12	850 \$
23.10.2019 12:00	23.10.2019 12:30	23.10.2019 10:49	18	518 \$
06.09.2019 17:00	06.09.2019 17:39	06.09.2019 15:27	16	610 \$
28.08.2019 18:00 *	28.08.2019 18:34	28.08.2019 16:19	12	650 \$
10.08.2019 11:00 *	10.08.2019 11:31	10.08.2019 09:17	11	671 \$
27.07.2019 10:00	27.07.2019 10:37	27.07.2019 08:23	13	616 \$
10.07.2019 11:00	10.07.2019 14:35	10.07.2019 12:18	19	591 \$
26.05.2019 19:00	26.05.2019 19:30	26.05.2019 17:14	10	602 \$
17.05.2019 03:00 *	17.05.2019 03:38	17.05.2019 01:26	13	1200 \$
02.04.2019 04:00	02.04.2019 04:39	02.04.2019 02:24	14	620 \$
22.06.2019 14:00 *	22.06.2019 14:36	22.06.2019 12:24	12	860 \$

Tabulka 2: Tabulka velkých pohybů stažených pro analýzu

	Poslední blok (UTC)	První blok (UTC)	Počet bloků	Rozdíl ceny
26.10.2019 1:00 *	19.10.2019 01:22	18.10.2019 23:33	12	5 \$
24.09.2019 18:00 *	17.09.2019 18:42	17.09.2019 16:32	16	7 \$
06.08.2019 10:00 *	30.07.2019 10:30	30.07.2019 8:29	11	8 \$
26.06.2019 20:00 *	19.06.2019 20:33	19.06.2019 18:24	21	25 \$
27.06.2019 16:00 *	20.06.2019 16:41	20.06.2019 14:19	16	25 \$
18.12.2019 22:00	12.12.2019 22:27	12.12.2019 20:44	14	3 \$
04.12.2019 13:00	27.11.2019 13:30	27.11.2019 11:24	12	25 \$
25.11.2019 12:00	18.11.2019 12:35	18.11.2019 10:26	7	24 \$
22.11.2019 10:00	15.11.2019 10:44	15.11.2019 08:31	15	57 \$
25.10.2019 15:00 *	18.10.2019 25:25	18.10.2019 13:26	16	8 \$
23.10.2019 12:00	16.10.2019 12:34	16.10.2019 10:19	14	72 \$
06.09.2019 17:00	30.08.2019 17:32	30.08.2019 15:23	20	48 \$
28.08.2019 18:00 *	21.08.2019 18:32	21.08.2019 16:23	20	37 \$
10.08.2019 11:00 *	03.08.2019 11:26	03.08.2019 09:26	20	22 \$
27.07.2019 10:00	20.07.2019 10:45	20.07.2019 08:21	10	2 \$
10.07.2019 11:00	03.07.2019 14:42	03.07.2019 12:26	17	55 \$
26.05.2019 19:00	19.05.2019 19:35	19.05.2019 17:27	14	38 \$
17.05.2019 03:00 *	10.05.2019 03:29	10.05.2019 01:19	10	53 \$
02.04.2019 04:00	26.03.2019 04:33	26.03.2019 02:23	17	2 \$
22.06.2019 14:00 *	15.06.2019 14:29	15.06.2019 12:23	14	46 \$

Tabulka 3: Tabulka malých pohybů stažených pro analýzu

analyzovanou vlastnost také uvedu tabulku se statistickými daty (minimální hodnota, maximální hodnota, průměrná hodnota, směrodatná odchylka, medián a statistické testy).

V této kapitole používám dvouvýběrové statistické testy o shodách středních hodnot a mediánů. Dále také používám Shapirův-Wilkův test pro ověření normality dat. Všechny tyto testy byly prováděny na hladině významnosti 5%. Nulová hypotéza u Shapirova-Wilkova testu říká, že data jsou z normálního rozdělení. Alternativní hypotéza říká opak. Co se týče testu shody středních hodnot (t-test), ten má nastavenou nulovou hypotézu tak, že střední hodnoty obou výběrů jsou shodné. Alternativní hypotézu jsem následně v jazyce R vybral takovou, která tvrdí, že střední hodnota velkého pohybu je větší než střední hodnota malého pohybu. U testu o shodě mediánu (Mannův-Whitneyho test) jsou nulová i alternativní hypotéza nastavená stejně s tou výjimkou, že se testuje medián namísto střední hodnoty. Uvedené hodnoty statistických testů v tabulkách vyjadřují p-hodnotu.

### 5.2.1 Vlastnosti společné pro všechny sítě

V posbíraných sítích se objevilo pár rysů, které jsou společné pro všechny analyzované sítě a to i napříč sítěmi s malými a velkými pohyby.

- Souvislost - Žádná ze sítí není souvislá. Ve všech sítích se nachází několik tisíc až desítek tisíc komponent souvislosti.
- Hustota - Všechny analyzované sítě měly hustotu blížící se nule. Tato vlastnost poukazuje na to, že mezi adresami existuje relativně málo transakcí.

### 5.2.2 Analýza vrcholů a hran

První vlastností statických sítí kterou jsem analyzoval byly počty vrcholů a počty hran. Důvodem této analýzy bylo odhalení, zda se u velkých pohybů do transakcí zapojuje více adres, nebo jestli mezi adresami probíhá vyšší počet transakcí než obvykle.

Tabulka 4 zobrazuje počty vrcholů a hran u jednotlivých sítí. Z této tabulky nevyplývá žádná závislost velikosti pohybu na počtu účastníků, jelikož pouze 11 z 20 případů ukazuje vyšší počet vrcholů u velkého pohybu. Ani u počtu hran se neprokázala spojitost výskytu velkého pohybu ceny Bitcoinu s vyšším počtem transakcí mezi uzly, jelikož desetkrát byl počet hran vyšší u velkého pohybu a desetkrát byla tato informace vyšší u malého pohybu. Neplatí ani předpoklad, že více vrcholů musí nutně znamenat více hran.

V Tabulce 5 jsou zapsány statistické hodnoty pro vrcholy a hrany. Z tabulky vyplývá, že všechny hodnoty s výjimkou směrodatné odchylky u počtu vrcholů ukazují vyšší hodnoty pro velké pohyby. Zajímavá je maximální hodnota počtu hran u velkých pohybů, která u jednoho vzorku přesáhla dva miliony. To má také za následek razantní nárůst průměrné hodnoty a směrodatné odchylky u počtů hran při velkém pohybu. Statistické testy nepotvrdily, že by velký pohyb byl charakteristický větším počtem vrcholů ani větším počtem hran.

	Vrcholy		Hrany	
	Velký pohyb	Malý pohyb	Velký pohyb	Malý pohyb
06.08.2019 10:00	<b>113195</b>	66891	<b>500941</b>	193293
24.09.2019 18:00	114374	<b>127610</b>	<b>290646</b>	257239
26.06.2019 20:00	<b>147714</b>	124476	<b>742839</b>	317784
26.10.2019 01:00	<b>70121</b>	58990	<b>252708</b>	139966
27.06.2019 16:00	122758	<b>138786</b>	570821	<b>793822</b>
04.12.2019 13:00	87798	<b>90609</b>	200819	<b>213742</b>
06.09.2019 17:00	128054	<b>141497</b>	245947	<b>374108</b>
18.12.2019 22:00	<b>141572</b>	108663	<b>408926</b>	296398
22.11.2019 10:00	<b>120040</b>	90840	<b>277943</b>	214411
23.10.2019 12:00	<b>101172</b>	90353	<b>256793</b>	235827
25.10.2019 15:00	91575	<b>117316</b>	185080	<b>323621</b>
25.11.2019 10:00	<b>76704</b>	52571	<b>190047</b>	115314
28.08.2019 18:00	103379	<b>144461</b>	21616	<b>276145</b>
10.08.2019 11:00	69791	<b>83829</b>	176052	<b>248600</b>
27.07.2019 10:00	69325	<b>74723</b>	181169	<b>187485</b>
10.07.2019 14:00	<b>132386</b>	105260	297377	<b>337419</b>
26.05.2019 19:00	76274	<b>92391</b>	174948	<b>208169</b>
17.05.2019 03:00	<b>116522</b>	74723	<b>2049044</b>	187485
02.04.2019 04:00	<b>98202</b>	75302	398085	<b>636450</b>
22.06.2019 14:00	<b>96542</b>	92391	<b>458435</b>	208169

Tabulka 4: Tabulka počtů vrcholů a hran

	Vrcholy		Hrany	
	Velký pohyb	Malý pohyb	Velký pohyb	Malý pohyb
Minimum	<b>69325</b>	52571	<b>174948</b>	115314
Maximum	<b>147714</b>	144461	<b>2049044</b>	793822
Průměr	<b>103874,9</b>	97584,1	<b>403776,8</b>	288272,4
Směrodatná odchylka	24293,6	<b>27537,7</b>	<b>416434,8</b>	162108,2
Medián	<b>102275,5</b>	91615,5	<b>267368,0</b>	242213,5
Shapirův-Wilkův test	0,438	0,400	« 0,0002	« 0,0002
T-test / Mannův-Whitneyho test	0,224		0,237	

Tabulka 5: Tabulka statistických hodnot pro vrcholy a hrany

	Smyčky		Vícenásobné hrany	
	Velký pohyb	Malý pohyb	Velký pohyb	Malý pohyb
06.08.2019 10:00	<b>12884</b>	8028	<b>106236</b>	35228
24.09.2019 18:00	10578	<b>10930</b>	<b>35272</b>	31360
26.06.2019 20:00	12764	<b>16315</b>	<b>79007</b>	51149
26.10.2019 01:00	7553	<b>10109</b>	<b>23887</b>	16596
27.06.2019 16:00	<b>13821</b>	11206	72587	<b>97661</b>
04.12.2019 13:00	9906	<b>11198</b>	26015	<b>26263</b>
06.09.2019 17:00	10155	<b>14944</b>	30219	<b>42330</b>
18.12.2019 22:00	<b>7853</b>	6699	<b>38083</b>	28000
22.11.2019 10:00	11593	<b>19459</b>	<b>50297</b>	39000
23.10.2019 12:00	12689	<b>15220</b>	30276	<b>37488</b>
25.10.2019 15:00	9455	<b>12056</b>	21908	<b>33555</b>
25.11.2019 10:00	<b>9355</b>	7647	<b>28867</b>	17536
28.08.2019 18:00	6580	<b>11055</b>	24874	<b>48895</b>
10.08.2019 11:00	12391	<b>20087</b>	24850	<b>42182</b>
27.07.2019 10:00	<b>11216</b>	11059	27147	<b>29160</b>
10.07.2019 14:00	18955	<b>21043</b>	52090	<b>57635</b>
26.05.2019 19:00	10637	<b>19372</b>	25613	<b>49752</b>
17.05.2019 03:00	10966	<b>11059</b>	<b>71605</b>	29160
02.04.2019 04:00	18095	<b>22389</b>	<b>90207</b>	84304
22.06.2019 14:00	11672	<b>19372</b>	43452	<b>49752</b>

Tabulka 6: Tabulka počtů smyček a vícenásobných hran

Jelikož data se kterými pracuji můžou obsahovat vícenásobné hrany a smyčky, rozhodl jsem se analyzovat, kolik hran patří právě mezi smyčky a vícenásobné hrany. Tuto informaci zachycuje Tabulka 6, která udává počet smyček a vícenásobných hran.

V Tabulce 7 jsou spočítána statistická data pro smyčky a vícenásobné hrany. Z té lze vidět, že všechny statistické hodnoty u smyček jsou větší pro malé pohyby. To ukazuje menší počet smyček u velkých pohybů, což znamená malý počet transakcí, které se vrací zpět odesílateli. I když tabulka smyček ukazuje, že v 15 z 20 případů je počet smyček vyšší u velkých pohybů, tak statistické testy neprokázaly žádný rozdíl mezi velkými a malými pohyby na základě počtu smyček ani na základě počtu vícenásobných hran.

### 5.2.3 Analýza stupňů

Další oblastí kterou jsem zkoumal byly stupně vrcholů. Nejprve jsem se zaměřil na průměrný stupeň. Ten je zachycen v Tabulce 8. Ani zde se neobjevil zásadní rozdíl mezi velkým a malým pohybem, jelikož jen v 11 z 20 případů byl u velkého pohybu vyšší průměrný stupeň.

Tabulka 9 obsahuje statistická data pro průměrný stupeň v sítích. Zde se až na medián všechny statistické hodnoty ukazují vyšší u velkých pohybů než u těch malých, přičemž směrodatná odchylka je opět pravděpodobně ovlivněna vysokou hodnotou maxima průměrného stupně

	Smyčky		Vícenásobné hrany	
	Velký pohyb	Malý pohyb	Velký pohyb	Malý pohyb
Minimum	6580	<b>6699</b>	<b>21908</b>	16596
Maximum	18955	<b>22389</b>	<b>106236</b>	97661
Průměr	11455,9	<b>13962,4</b>	42124,6	<b>42350,3</b>
Směrodatná odchylka	3063,9	<b>4875,1</b>	<b>25321,5</b>	20076,6
Medián	11091	<b>11631</b>	32774	<b>38224</b>
Shapiro-Wilkův test	0,087	0,072	0,002	« 0,012
T-test / Mannův-Whitneyho test	0,970		0,622	

Tabulka 7: Tabulka statistických hodnot pro smyčky a vícenásobné hrany

	Velký pohyb	Malý pohyb
06.08.2019 10:00	<b>8,85</b>	5,78
24.09.2019 18:00	<b>5,08</b>	4,03
26.06.2019 20:00	<b>10,06</b>	5,11
26.10.2019 01:00	<b>7,21</b>	4,75
27.06.2019 16:00	9,30	<b>11,44</b>
04.12.2019 13:00	4,58	<b>4,72</b>
06.09.2019 17:00	3,84	<b>5,29</b>
18.12.2019 22:00	<b>5,78</b>	5,46
22.11.2019 10:00	4,63	<b>4,72</b>
23.10.2019 12:00	5,08	<b>5,22</b>
25.10.2019 15:00	4,04	<b>5,52</b>
25.11.2019 10:00	<b>4,96</b>	4,39
28.08.2019 18:00	<b>4,20</b>	3,82
10.08.2019 11:00	5,05	<b>5,93</b>
27.07.2019 10:00	<b>5,23</b>	5,02
10.07.2019 14:00	4,49	<b>6,41</b>
26.05.2019 19:00	<b>4,59</b>	4,51
17.05.2019 03:00	<b>35,17</b>	5,02
02.04.2019 04:00	8,11	<b>16,90</b>
22.06.2019 14:00	<b>9,50</b>	4,51

Tabulka 8: Tabulka stupňů vrcholů



	Velký pohyb	Malý pohyb
Minimum	<b>3,84</b>	3,82
Maximum	<b>35,17</b>	16,90
Průměr	<b>7,49</b>	5,93
Směrodatná odchylka	<b>6,82</b>	3,02
Medián	5,08	<b>8,06</b>
Shapirův-Wilkův test	« 0,001	« 0,001
Mannův-Whitneyho test	0,338	

Tabulka 9: Tabulka statistických hodnot pro stupeň vrcholů

u velkých pohybů. Vyšší medián při menším maximu znamená rovnoměrnější rozdělení stupňů mezi vrcholy. Statistické testy neprokázaly rozdíl v mělých a velkých pohybech na základě průměrných stupňů uzlů.

Následovala analýza distribuce stupňů, která by mohla poodhalit strukturu sítě. Na Obrázku 7 jsou příklady distribucí, které se u sítí vyskytovaly. Osy v tomto obrázku jsou v logaritmickém měřítku. Všechny analyzované distribuce stupňů měly velice podobný tvar. Jejich tvar na pohled připomíná mocninné rozdělení, avšak ten se použitím Kolmogorova-Smirnovova testu neprokázal, jelikož na hladině významnosti 5% vždy zamítnul nulovou hypotézu, že distribuce patří do mocninného rozdělení.

Distribuce stupňů však ukázala, že se jedná o síť, kde drtivá většina uzlů má nízký stupeň, ale existuje i pár uzlů, které se chovají jako HUBy ať už ve smyslu, že odesílají hodně transakcí, nebo přijímají hodně transakcí nebo obojí. Těmto centrům se budu věnovat dále detailněji v pozdější části práce.

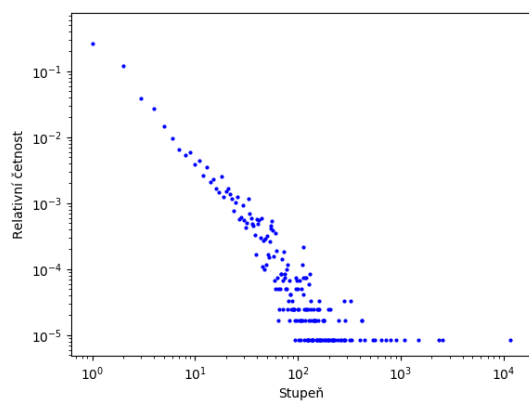
Jediné rozdíly které se mezi distribucemi objevovaly, byly odchylky od pomyslné přímky, kterou distribuce kopírují. Obrázky 7(a) a 7(b) jsou distribuce stupňů u velkých pohybů. Právě u obrázku 7(b) je vidět poměrně velká část bodů, která se odchyluje od mocninného rozdělení narozdíl od obrázku 7(a). Stejný případ lze pozorovat i u obrázků 7(c) a 7(d), kde se stejná situace vyskytuje i u malých pohybů.

Bohužel tedy ani ze samotných distribucí nelze určit, zda se jedná o malý či velký pohyb, jelikož dané distribuce nevykazují žádné typické chování pro daný pohyb.

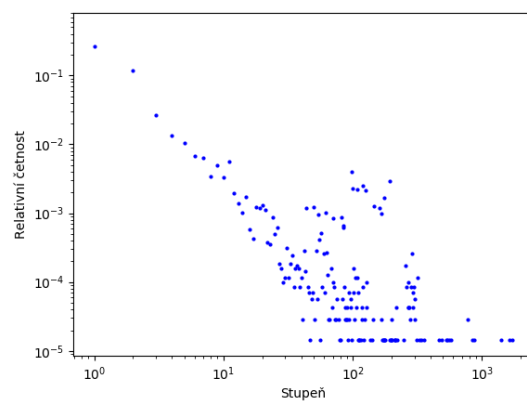
#### 5.2.4 Analýza vzdáleností

Pokračoval jsem analýzou vzdáleností. Důvodem analýzy této oblasti bylo zjistit, zda u velkých či malých pohybů nedochází k návaznosti jednotlivých transakcí, což by se ukázalo na delších cestách v síti.

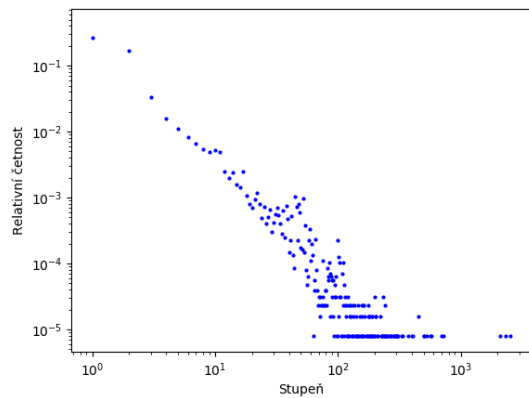
První vlastností z této oblasti byl analyzován průměr sítě, což je metrika zachycující nejdelší nejkratší cestu v dané síti. Data jsou vidět v Tabulce 10. Je vidět, že když vezmeme v potaz počty vrcholů v sítích (v řádech desetitisíců), průměry jsou poměrně malé, nepřesahující hodnotu



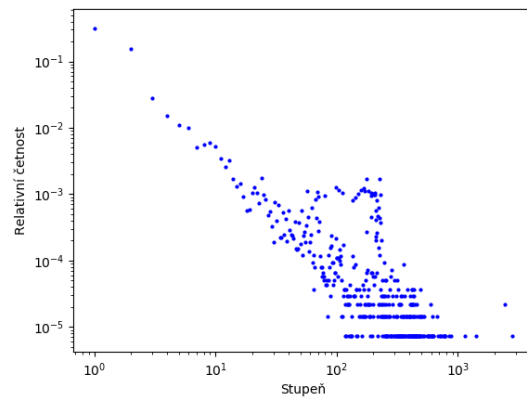
(a) Distribuce stupňů vrcholů z velkého pohybu bez odchylek



(b) Distribuce stupňů vrcholů z velkého pohybu s odchylkami



(c) Distribuce stupňů vrcholů z malého pohybu bez odchylek



(d) Distribuce stupňů vrchol z malého pohybu s odchylkami

Obrázek 7: Příklad distribucí stupňů

	Velký pohyb	Malý pohyb
06.08.2019 10:00	<b>57</b>	31
24.09.2019 18:00	<b>82</b>	71
26.06.2019 20:00	<b>63</b>	44
26.10.2019 01:00	<b>92</b>	43
27.06.2019 16:00	37	<b>65</b>
04.12.2019 13:00	<b>49</b>	39
06.09.2019 17:00	58	<b>61</b>
18.12.2019 22:00	<b>91</b>	44
22.11.2019 10:00	<b>61</b>	60
23.10.2019 12:00	44	<b>61</b>
25.10.2019 15:00	<b>60</b>	56
25.11.2019 10:00	44	<b>61</b>
28.08.2019 18:00	42	<b>66</b>
10.08.2019 11:00	125	125
27.07.2019 10:00	<b>84</b>	58
10.07.2019 14:00	40	<b>41</b>
26.05.2019 19:00	41	<b>109</b>
17.05.2019 03:00	<b>91</b>	58
02.04.2019 04:00	<b>56</b>	28
22.06.2019 14:00	54	<b>109</b>

Tabulka 10: Tabulka průměrů sítí

125 přeskoků. Důvodem tak malých průměrů sítí může být i fakt, že sítě nejsou hustě propojeny a tvoří obrovské množství malých silně propojených komponent. Počty propojených komponent je možné vidět v Tabulce 14.

Vypočtená statistická data pro průměr sítě jsou v Tabulce 11. Ani zde statistické testy nepotvrdily rozdíl mezi velkými a malými pohyby na základě průměrů v sítích.

Po průměru sítě následovala analýza délky průměrné cesty. Ta je vidět v Tabulce 12. Platí stejná věc co u průměru sítí a sice, že v poměru s počtem vrcholů jsou délky průměrných cest poměrně malé. To indikuje velký počet kratších cest a velice malý počet cest delších. Opět ani zde se neukázal větší rozdíl mezi malými a velkými pohyby.

Tabulka 13 ukazuje statistické hodnoty pro průměrnou délku cesty. Ani zde statistické testy neprokázaly odlišnosti mezi průměrnou délkou cesty u malých a velkých pohybů

### 5.2.5 Analýza komponent v sítích

V této práci už jsem se zmínil o tom, že je síť hodně rozdělena do malých komponent souvislosti. Proto následovalo přesnější zkoumání silně a slabě propojených komponent. Počty těchto komponent jsou vidět v Tabulce 14. Z tabulky lze vidět, že uzly mezi sebou skoro vůbec nejsou silně propojeny, jelikož počet silně propojených komponent se blíží počtu vrcholů v síti. Co se

	Velký pohyb	Malý pohyb
Minimum	<b>37</b>	28
Maximum	125	125
Průměr	<b>63,7</b>	61,5
Směrodatná odchylka	23,1	<b>25,8</b>
Medián	57,5	<b>59,0</b>
Shapirův-Wilkův test	0,018	0,007
Mannův-Whitneyho test	0,430	

Tabulka 11: Tabulka statistických hodnot pro průměr sítě

	Velký pohyb	Malý pohyb
06.08.2019 10:00	<b>8,66</b>	4,56
24.09.2019 18:00	<b>9,97</b>	9,50
26.06.2019 20:00	6,40	<b>9,16</b>
26.10.2019 01:00	<b>7,76</b>	5,23
27.06.2019 16:00	6,53	<b>8,78</b>
04.12.2019 13:00	<b>11,14</b>	8,30
06.09.2019 17:00	<b>10,68</b>	10,45
18.12.2019 22:00	9,30	<b>9,55</b>
22.11.2019 10:00	10,36	<b>10,86</b>
23.10.2019 12:00	10,01	<b>12,26</b>
25.10.2019 15:00	10,56	<b>10,71</b>
25.11.2019 10:00	<b>10,63</b>	4,53
28.08.2019 18:00	7,68	<b>9,53</b>
10.08.2019 11:00	<b>11,31</b>	10,03
27.07.2019 10:00	<b>9,83</b>	6,56
10.07.2019 14:00	8,09	<b>8,24</b>
26.05.2019 19:00	8,82	<b>9,34</b>
17.05.2019 03:00	<b>6,79</b>	6,56
02.04.2019 04:00	<b>7,79</b>	5,91
22.06.2019 14:00	8,10	<b>9,34</b>

Tabulka 12: Tabulka délky průměrných cest

	Velký pohyb	Malý pohyb
Minimum	<b>6,40</b>	4,53
Maximum	11,31	<b>12,26</b>
Průměr	<b>9,02</b>	8,47
Směrodatná odchylka	1,57	<b>2,20</b>
Medián	9,06	<b>9,25</b>
Shapirův-Wilkův test	0,217	0,159
T-test	0,185	

Tabulka 13: Tabulka statistických hodnot pro průměrnou délku cesty

týče slabé konektivity, tam jsou počty komponent řádově nižší, což znamená síť sice není silně propojena, ale mezi skupinami vrcholů existují alespoň jednostranné vazby na ostatní skupiny vrcholů.

Ani v této vlastnosti se nepodařilo rozdělit síť do malého a velkého pohybu, jelikož v obou případech jedenáctkrát z dvaceti byly počty komponent vyšší u velkých pohybů než u malých pohybů.

Tabulka 15 ukazuje statistická data pro počty silně a slabě propojených komponent. Ani zde nelze pozorovat odlišnosti pro hodnoty počtů komponent mezi malým a velkým pohybem na základě statistických testů.

V souvislosti s počtem komponent jsem se rozhodl dále analyzovat i velikost největší komponenty souvislosti. Tímto by se dalo zjistit, zda se u velkých či malých pohybů netvoří větší komunity uzlů. Tyto velikosti jsou v Tabulce 16. Zde je opět vidět rozdíl v hodnotách někdy až o dva řády. Těmito hodnotami se utvrdilo mé dřívější tvrzení, že síť je z velké části propojena pouze jednosměrnými hranami.

Z hodnot největší silně propojené komponenty můžeme vypočítat, že ve 14 z 20 případů je u velkých pohybů největší silně propojená komponenta větší než je tomu u malých pohybů. Z toho by šlo usoudit, že u velkých pohybů existují větší skupiny uzlů, které figurují jak v roli odesílatele, tak v roli příjemce Bitcoinů. Takové chování by se dalo odůvodnit posíláním Bitcoinů tam a zpět mezi dvěma či více adresami. U největších slabě propojených komponent takové chování není přítomno.

I pro velikosti silných a slabých komponent jsem počítal statistická data. Ty jsou v Tabulce 17. U silných komponent je sice vidět, že všechny hodnoty statistických dat jsou vyšší u velkých pohybů, ale statistické testy neprokázaly rozdíl mezi velkými a malými pohyby.

### 5.2.6 Analýza shlukovacího koeficientu a betweenness centrality

V této podkapitole jsem se zaměřil na analýzu shlukovacího koeficientu a betweenness centrality. Tato část navazuje na analýzy vzdáleností a analýzy komponent. Data shlukovacích koeficientů je v Tabulce 18.

	Silné komponenty		Slabé komponenty	
	Velký pohyb	Malý pohyb	Velký pohyb	Malý pohyb
06.08.2019 10:00	<b>111597</b>	66530	<b>10238</b>	5063
24.09.2019 18:00	113076	<b>126036</b>	9208	<b>10944</b>
26.06.2019 20:00	<b>146025</b>	122969	<b>12627</b>	10467
26.10.2019 01:00	<b>69737</b>	58794	<b>6511</b>	5426
27.06.2019 16:00	121075	<b>137298</b>	<b>10327</b>	8328
04.12.2019 13:00	87424	<b>89791</b>	8107	<b>8346</b>
06.09.2019 17:00	125771	<b>139628</b>	<b>11520</b>	10733
18.12.2019 22:00	<b>140529</b>	108380	<b>11587</b>	8847
22.11.2019 10:00	<b>117197</b>	89938	<b>8712</b>	6958
23.10.2019 12:00	<b>99500</b>	89287	8214	<b>8420</b>
25.10.2019 15:00	90337	<b>115298</b>	7202	<b>8913</b>
25.11.2019 10:00	<b>75952</b>	52263	<b>7553</b>	6814
28.08.2019 18:00	102733	<b>143021</b>	9312	<b>10164</b>
10.08.2019 11:00	68885	<b>82873</b>	6303	<b>6793</b>
27.07.2019 10:00	68134	<b>74123</b>	5763	<b>5766</b>
10.07.2019 14:00	<b>130440</b>	102673	<b>12267</b>	9217
26.05.2019 19:00	75380	<b>91677</b>	6882	<b>9685</b>
17.05.2019 03:00	<b>115487</b>	74123	<b>7412</b>	5766
02.04.2019 04:00	<b>96419</b>	73988	<b>8712</b>	6080
22.06.2019 14:00	<b>95140</b>	91677	8287	<b>9685</b>

Tabulka 14: Tabulka počtů silně a slabě propojených komponent

	Silné komponenty		Slabé komponenty	
	Velký pohyb	Malý pohyb	Velký pohyb	Malý pohyb
Minimum	<b>68134</b>	52263	<b>5763</b>	5063
Maximum	<b>146025</b>	143021	<b>12627</b>	10944
Průměr	<b>102541,9</b>	96518,2	<b>8837,2</b>	8120,8
Směrodatná odchylka	23937,6	<b>27097,9</b>	<b>2028,0</b>	1900,1
Medián	<b>101116,5</b>	90807,5	<b>8499,5</b>	8383,0
Shapirův-Wilkův test	0,475	0,409	0,382	« 0,195
T-test	0,230		0,128	

Tabulka 15: Tabulka statistických hodnot pro počty silně a slabě propojených komponent

	Silné komponenty		Slabé komponenty	
	Velký pohyb	Malý pohyb	Velký pohyb	Malý pohyb
06.08.2019 10:00	<b>1388</b>	189	<b>66325</b>	42166
24.09.2019 18:00	1053	<b>1140</b>	71760	<b>76184</b>
26.06.2019 20:00	<b>1582</b>	1387	<b>92294</b>	73474
26.10.2019 01:00	<b>103</b>	50	<b>36730</b>	32385
27.06.2019 16:00	<b>1382</b>	1333	68975	<b>98196</b>
04.12.2019 13:00	106	<b>694</b>	51389	<b>53464</b>
06.09.2019 17:00	<b>2024</b>	1625	74224	<b>87468</b>
18.12.2019 22:00	<b>767</b>	155	<b>85163</b>	65736
22.11.2019 10:00	<b>2578</b>	692	<b>80082</b>	56982
23.10.2019 12:00	<b>1179</b>	497	<b>59688</b>	49483
25.10.2019 15:00	931	<b>1750</b>	56589	<b>77973</b>
25.11.2019 10:00	<b>643</b>	237	<b>42288</b>	23225
28.08.2019 18:00	423	<b>1186</b>	54224	<b>95989</b>
10.08.2019 11:00	762	<b>796</b>	39284	<b>52853</b>
27.07.2019 10:00	<b>1034</b>	424	42543	<b>46647</b>
10.07.2019 14:00	1728	<b>2346</b>	<b>81222</b>	64971
26.05.2019 19:00	<b>649</b>	619	45056	<b>47158</b>
17.05.2019 03:00	<b>844</b>	424	<b>80591</b>	46647
02.04.2019 04:00	<b>1678</b>	1166	<b>56145</b>	49472
22.06.2019 14:00	<b>1291</b>	619	<b>59569</b>	47158

Tabulka 16: Tabulka velikostí největší silně a slabě propojené komponenty

	Silné komponenty		Slabé komponenty	
	Velký pohyb	Malý pohyb	Velký pohyb	Malý pohyb
Minimum	<b>103</b>	50	<b>36730</b>	23225
Maximum	<b>2578</b>	2346	92294	<b>98196</b>
Průměr	<b>1107,3</b>	866,5	<b>62207,1</b>	59381,6
Směrodatná odchylka	<b>623,3</b>	608,9	16645,2	<b>20221,1</b>
Medián	<b>1043,5</b>	693,0	<b>59628,5</b>	53158,5
Shapiro-Wilkův test	0,870	0,249	0,501	0,355
T-test	0,112		0,355	

Tabulka 17: Tabulka statistických hodnot pro velikosti největších propojených komponent

	Velký pohyb	Malý pohyb
06.08.2019 10:00	<b>0,019</b>	0,015
24.09.2019 18:00	0,011	<b>0,012</b>
26.06.2019 20:00	<b>0,016</b>	0,014
26.10.2019 01:00	0,010	<b>0,011</b>
27.06.2019 16:00	<b>0,012</b>	0,011
04.12.2019 13:00	0,012	<b>0,016</b>
06.09.2019 17:00	0,011	<b>0,012</b>
18.12.2019 22:00	<b>0,0105</b>	0,011
22.11.2019 10:00	<b>0,018</b>	0,012
23.10.2019 12:00	0,015	<b>0,022</b>
25.10.2019 15:00	0,011	<b>0,013</b>
25.11.2019 10:00	<b>0,014</b>	0,013
28.08.2019 18:00	0,011	<b>0,012</b>
10.08.2019 11:00	0,012	<b>0,016</b>
27.07.2019 10:00	<b>0,014</b>	0,013
10.07.2019 14:00	0,011	<b>0,014</b>
26.05.2019 19:00	<b>0,014</b>	0,013
17.05.2019 03:00	<b>0,015</b>	0,013
02.04.2019 04:00	0,019	<b>0,022</b>
22.06.2019 14:00	0,011	<b>0,013</b>

Tabulka 18: Tabulka shlukovacích koeficientů



	Velký pohyb	Malý pohyb
Minimum	0,010	<b>0,011</b>
Maximum	0,019	<b>0,022</b>
Průměr	0,0136	<b>0,0140</b>
Směrodatná odchylka	0,0028	<b>0,0031</b>
Medián	0,013	0,013
Shapirův-Wilkův test	0,019	0,002
Mannův-Whitneyho test	0,678	

Tabulka 19: Tabulka statistických hodnot pro shlukovací koeficient

Vypočítaná statistická data pro shlukovací koeficient jsou v Tabulce 19. Ani u shlukovacího koeficientu se neprokázal rozdíl mezi hodnotami u malých a velkých pohybů podle statistických testů.

Co se týče betweenness centrality, tam jsem prováděl analýz více. Nejprve jsem analyzoval celkovou míru betweenness centrality pro celou síť. Ta je vidět v Tabulce 20. Opět lze upozorovat velice nízké hodnoty betweenness centrality, které však mají větší odchylku mezi jednotlivými sítěmi než je tomu u shlukovacího koeficientu.

U betweenness centrality je možné upozorovat, že ve 14 z 20 případů je spojena vyšší betweenness centralita s větším pohybem. To by znamenalo, že v síti existují uzly, skrze které teče velké množství transakcí. Takové uzly by se daly označit za centra v síti (HUBy), které spojují danou síť v celek. Zajímavou informací která z analýzy vyplynula, je poměr uzlů, které mají nulovou betweenness centralitu, což znamená, že skrz ně nevede ani jedna nejkratší cesta. Tato hodnota se u žádné sítě nedostala pod 75%. Z toho vyplývá, že v síti je obrovský počet uzlů, přes které neputují žádné bitcoiny a jedná se o uzly, které pouze posílají nebo pouze přijímají bitcoiny. V jednom případě se tato hodnota vyšplhala až k 90% z celkových uzlů.

V souvislosti s globální betweenness centralitou jsem analyzoval i lokální hodnoty této charakteristiky. U sítí kde betweenness centralita překročila hodnotu 0.01 jsem spočítal tuto charakteristiku pro všechny uzly v síti a zkoumal jsem uzly, jejichž hodnota betweenness centrality byla v rámci sítě nejvyšší.

Ve všech případech se jednalo o uzel s tou stejnou adresou, která patří kryptoburze Binance. Dá se tedy říct, že burza Binance v mém případě tvoří v sítích most, který spojuje více izolovaných komponent k sobě skrze nejkratší cesty.

Tabulka 21 obsahuje statistická data pro betweenness centralitu i pro procentuální zastoupení uzlů s nulovou betweenness centralitou. Zde poprvé statistické testy prokázaly, že betweenness centralita u velkých pohybů není shodná s betweenness centralitou u malých pohybů, ale je vyšší. To znamená, že síť s velkými pohyby má vyšší betweenness centralitu, což znamená, že obsahují uzly, přes které vede výrazně více nejkratších cest než u malých pohybů, nebo obsahují více uzlů, skrze které vede více nejkratších cest. To by pak znamenalo více uzlů, které přeposílají

	Betweenness centralita		% uzlů s 0 betweenness centralitou	
	Velký pohyb	Malý pohyb	Velký pohyb	Malý pohyb
06.08.2019 10:00	<b>0,0117</b>	0,0004	83,2	<b>91,4</b>
24.09.2019 18:00	<b>0,0084</b>	0,0072	80,1	<b>80,5</b>
26.06.2019 20:00	<b>0,0145</b>	0,0094	<b>82,8</b>	82,0
26.10.2019 01:00	<b>0,0024</b>	0,0004	<b>85,3</b>	83,9
27.06.2019 16:00	<b>0,0117</b>	0,0110	82,1	<b>82,6</b>
04.12.2019 13:00	0,0004	<b>0,0072</b>	<b>83,9</b>	81,4
06.09.2019 17:00	0,0088	<b>0,0103</b>	78,9	<b>81,5</b>
18.12.2019 22:00	<b>0,0053</b>	0,0019	82,7	<b>84,4</b>
22.11.2019 10:00	<b>0,0150</b>	0,0056	80,3	<b>82,3</b>
23.10.2019 12:00	<b>0,0078</b>	0,0033	81,3	<b>83,4</b>
25.10.2019 15:00	0,0072	<b>0,0094</b>	<b>82,4</b>	77,2
25.11.2019 10:00	<b>0,0072</b>	0,0002	82,7	<b>85,5</b>
28.08.2019 18:00	0,0056	<b>0,0057</b>	<b>83,0</b>	81,1
10.08.2019 11:00	0,0058	<b>0,0088</b>	<b>82,9</b>	80,9
27.07.2019 10:00	<b>0,0073</b>	0,0018	82,9	<b>85,3</b>
10.07.2019 14:00	<b>0,0122</b>	0,0110	<b>82,0</b>	80,8
26.05.2019 19:00	<b>0,0064</b>	0,0057	82,2	<b>83,9</b>
17.05.2019 03:00	<b>0,0087</b>	0,0018	<b>88,4</b>	85,3
02.04.2019 04:00	0,0049	<b>0,0065</b>	80,5	<b>84,4</b>
22.06.2019 14:00	<b>0,0172</b>	0,0057	83,5	<b>83,9</b>

Tabulka 20: Tabulka údajů související s betweenness centralitou

	Betweenness centralita		% uzlů s 0 betweenness centralitou	
	Velký pohyb	Malý pohyb	Velký pohyb	Malý pohyb
Minimum	<b>0,0004</b>	0,0002	<b>78,9</b>	77,2
Maximum	<b>0,0172</b>	0,0110	88,4	<b>91,4</b>
Průměr	<b>0,0084</b>	0,0057	82,6	<b>83,1</b>
Směrodatná odchylka	<b>0,0042</b>	0,0037	2,0	<b>2,8</b>
Medián	<b>0,0075</b>	0,0057	82,7	<b>83,0</b>
Shapirův-Wilkův test	0,696	0,112	0,055	0,070
T-test	0,017		0,750	

Tabulka 21: Statistika betweenness centrality (BC) a zastoupení uzlů s nulovou BC

transakce dál, nebo uzly, které přeposílají hodně transakcí dále. U procentuálního zastoupení uzlů s nulovou betweenness centralitou se podobná vlastnost neprokázala.

### 5.2.7 Stupňová asortativita a reciprocita hran

Posledními vlastnostmi, které jsem zkoumal byly stupňová asortativita a reciprocita hran. Důvodem zkoumání stupňové asortativity bylo odhalit, zda se uzly v síti spojují s uzly s podobným stupněm. Tímto by se dalo zjistit, zda se centrální uzly spojují navzájem nebo se spíše spojují s okrajovými uzly s malým stupněm. Reciprocita hran by mohla odhalit, zda se u sítí s velkým pohybem vyskytují hrany oběma směry, či se naopak vyskytují spíše jednosměrné transakce.

Tabulka stupňové asortativity je vidět v Tabulce 22. Z těchto hodnot můžeme vypočítat výrazné kolísání mezi jednotlivými sítěmi. Hodnoty naměřené na mém vzorku však neklesají vysoko pod 0, což indikuje, že se v síti nespojují centrální uzly s velkým stupněm s těmi okrajovými. Nastávají vesměs dvě situace. Buďto neexistuje žádné pravidlo, že by se podobné uzly spojovaly hranami (to odpovídá hodnotám asortativity okolo nuly), nebo se uzly s podobným stupněm právě spojují hranami (to platí pro hodnoty blíží se 1). Nenalezl jsem však pravidlo, které by podle stupňové asortativity dokázalo určit, zda se jedná o síť s velkým či malým pohybem.

V Tabulce 23 jsou zaznamenány statistické hodnoty pro stupňovou asortativitu. Z té lze vypočítat, že medián i průměr se pohybují okolo nuly, což by naznačovalo, že neexistuje korelace spojování uzlů s podobným stupněm. Statistické testy ani zde neprokázaly rozdíl mezi hodnotami stupňové asortativity u velkých a malých pohybů.

Úplně poslední charakteristikou kterou jsem zkoumal, byla reciprocita hran. Ta je v Tabulce 24. Z ní je vidět, že hrany často opětovány nejsou, přičemž poměr hran, ke kterým existuje hrana i v opačném směru je maximálně jedno procento. Výsledkem této analýzy je však fakt, že pouze u 5 z 20 případů byla u velkého pohybu vyšší reciprocita hran, než u malého. To by znamenalo, že velké pohyby obsahují více jednosměrných transakcí, než ty malé. Z tohoto faktu vyplývá, že

	Velký pohyb	Malý pohyb
06.08.2019 10:00	<b>0,364</b>	-0,059
24.09.2019 18:00	<b>-0,021</b>	-0,028
26.06.2019 20:00	-0,100	<b>0,654</b>
26.10.2019 01:00	<b>-0,031</b>	-0,067
27.06.2019 16:00	0,097	<b>0,136</b>
04.12.2019 13:00	0,011	<b>0,014</b>
06.09.2019 17:00	<b>0,165</b>	-0,060
18.12.2019 22:00	-0,007	<b>0,142</b>
22.11.2019 10:00	-0,068	<b>0,568</b>
23.10.2019 12:00	0,052	<b>0,161</b>
25.10.2019 15:00	<b>0,071</b>	0,004
25.11.2019 10:00	0,053	<b>0,218</b>
28.08.2019 18:00	<b>-0,015</b>	-0,101
10.08.2019 11:00	<b>0,293</b>	0,059
27.07.2019 10:00	<b>0,258</b>	0,006
10.07.2019 14:00	-0,047	<b>0,019</b>
26.05.2019 19:00	-0,028	<b>0,526</b>
17.05.2019 03:00	-0,098	<b>0,006</b>
02.04.2019 04:00	<b>0,070</b>	0,014
22.06.2019 14:00	0,154	<b>0,526</b>

Tabulka 22: Tabulka stupňové asortativity

	Velký pohyb	Malý pohyb
Minimum	-0,1	-0,1
Maximum	0,364	<b>0,654</b>
Průměr	0,059	<b>0,138</b>
Směrodatná odchylka	0,130	<b>0,237</b>
Medián	<b>0,032</b>	0,017
Shapiro-Wilkův test	0,055	0,008
Mannův-Whitneyho test	0,780	

Tabulka 23: Tabulka statistických hodnot pro stupňovou asortativitu

	Velký pohyb	Malý pohyb
06.08.2019 10:00	0,0013	<b>0,0016</b>
24.09.2019 18:00	0,0028	<b>0,0049</b>
26.06.2019 20:00	0,0008	<b>0,0015</b>
26.10.2019 01:00	0,0015	<b>0,0017</b>
27.06.2019 16:00	<b>0,0016</b>	0,0007
04.12.2019 13:00	0,0028	<b>0,0035</b>
06.09.2019 17:00	<b>0,0027</b>	0,0017
18.12.2019 22:00	0,0011	<b>0,0017</b>
22.11.2019 10:00	<b>0,0032</b>	0,0027
23.10.2019 12:00	<b>0,0042</b>	0,0026
25.10.2019 15:00	<b>0,0037</b>	0,0024
25.11.2019 10:00	0,0023	<b>0,0050</b>
28.08.2019 18:00	0,0010	<b>0,0017</b>
10.08.2019 11:00	0,0026	<b>0,0031</b>
27.07.2019 10:00	0,0072	<b>0,0079</b>
10.07.2019 14:00	0,0019	<b>0,0023</b>
26.05.2019 19:00	0,0035	<b>0,0104</b>
17.05.2019 03:00	0,0002	<b>0,0079</b>
02.04.2019 04:00	0,0034	<b>0,0037</b>
22.06.2019 14:00	0,0012	<b>0,0104</b>

Tabulka 24: Tabulka reciprocity hran

nedochází k opakovaným pohybům od jednoho subjektu ke druhému a pokud ano, tak pouze v případě, že si subjekty pro každé transakce generují nové adresy.

Tabulka 25 obsahuje statistické hodnoty pro reciprocitu hran. Z ní lze vidět, že se její hodnoty blíží nule, což znamená, že hrany nejsou obousměrné ani u malých ani u velkých pohybů. Mannův-Whitneyho test pak neprokázal odlišnost hodnot reciprocity hran u velkých a malých pohybů.

### 5.3 Dynamická analýza

Dalším krokem mé práce byla dynamická analýza transakcí v síti Bitcoin. Mou snahou tedy bylo zachytit vývoj chování Bitcoinu z pohledu komplexních sítí v čase. Při vybírání modelu pro temporální síť jsem narazil na dva způsoby.

První způsob uvedený v práci [10] modeluje temporální síť pomocí několika oddělených sítí v závislosti na čase. Autoři si určili 5 časových období, ze kterých sestrojili 5 temporálních sítí a následně porovnávali vlastnosti mezi nimi. Na tomto modelu je pak možné provádět analýzy, které je možno provádět na klasických grafech.

Druhý způsob uvedený v práci [26] modeluje temporální síť pomocí grafů vyššího stupně, kdy jeden vrchol v grafu by nereprezentoval jeden uzel v Bitcoinové síti, ale reprezentoval by

	Velký pohyb	Malý pohyb
Minimum	0,0002	0,0002
Maximum	0,0072	<b>0,0104</b>
Průměr	0,0025	<b>0,0039</b>
Směrodatná odchylka	0,0016	<b>0,0030</b>
Medián	0,0025	<b>0,0027</b>
Shapirův-Wilkův test	0,041	0,001
Mannův-Whitneyho test	0,932	

Tabulka 25: Tabulka statistických hodnot pro stupňovou asortativitu

Označení sítě	Datum
S1	17.05.2019 03:00
S2	24.09.2019 18:00
S3	25.10.2019 15:00
S4	26.06.2019 20:00
S5	26.10.2019 01:00
S6	27.06.2019 16:00
S7	06.08.2019 10:00
S8	10.08.2019 11:00
S9	28.08.2019 18:00
S10	22.06.2019 14:00

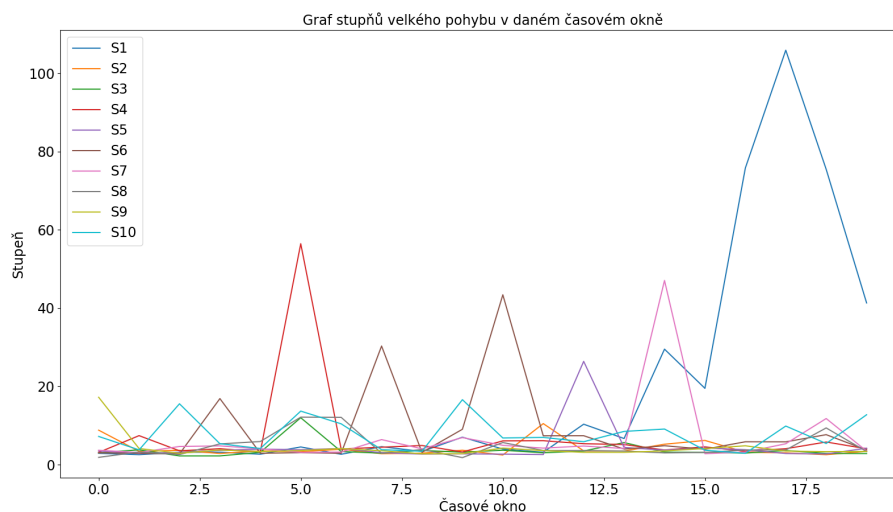
Tabulka 26: Tabulka označení temporální sítě a příslušného datumu

hranu mezi dvěma vrcholy. V mém případě by jeden uzel v grafu vyššího stupně reprezentoval dvojici uzlů v Bitcoinové síti, mezi kterými proběhla transakce. Tento model pak umožňuje efektivní analýzu cest v temporálních sítích a to včetně centralit bztahující se k cestám v grafu.

V mé práci jsem využil první mnou uvedený model temporálních sítí o dvaceti časových oknech, kdy jeden blok odpovídal jednomu časovému oknu. Bylo to z důvodu toho, že jsem chtěl provést analýzu stejných vlastností jako u statických grafů a zachytit jejich vývoj v čase.

V následujících tabulkách budou jednotlivé sítě identifikovány číslem místo datumu ve tvaru S1 VP, S2 MP atd. Zkratky VP a MP znamenají velký, respektive malý pohyb. Důvodem tohoto značení je úspora místa v tabulce. Tabulka 26 pak ukazuje, které datum patří ke které síti.

V této kapitole jsou obrázky částí sítí pro porovnání situace, kdy došlo k nárůstu průměrného stupně se situací, kdy byl průměrný stupeň v klidových hodnotách. Kompletní obrázky jsou k nalezení v příloze A. Tabulky 31 až 34 v příloze A zachycují počty vrcholů a hran v jednotlivých temporálních sítích v určitém časovém okně.



Obrázek 8: Průběh průměrného stupně uzlů u velkých pohybu.

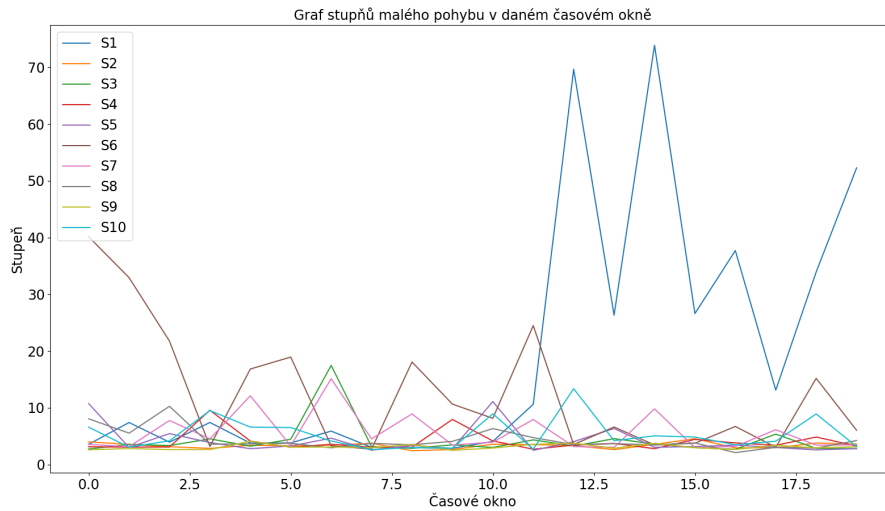
### 5.3.1 Analýza stupňů

První věc kterou jsem u temporálních sítí analyzoval byla analýza průměrného stupně v každém časovém okně dané temporální sítě. Kompletní tabulku lze vidět v Tabulkách 35, 36 v příloze A.

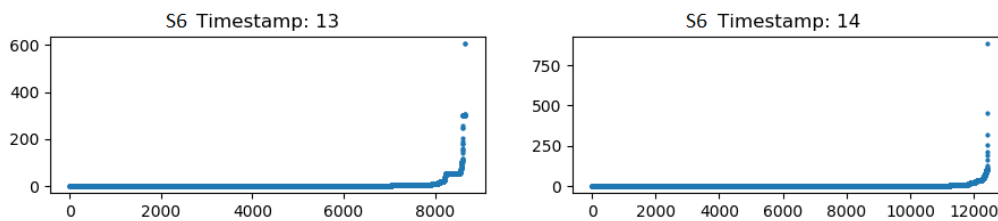
Z tabulky lze vypožorovat, že ve většině případů dojde v určitém časovém okně k razantnímu nárůstu průměrného stupně v síti. Co se týče maximální hodnoty stupně, tato hodnota je v 8 z 10 případů vyšší u velkého pohybu než u pohybu malého. To indikuje, že v určitém bloku razantně vzroste počet transakcí nebo se vyskytne více transakcí s mnoha uzly na vstupu nebo výstupu. Tento nárůst má však kromě jednoho případu podobu jednorázového nárůstu a následného pádu do klidových hodnot, které se pohybují okolo hodnoty 3,5. To že nastal nárůst stupně považuji jeho překročením klidové hodnoty minimálně o dvojnásobek.

Na Obrázku 8 lze vidět průběh stupňů ve všech 10 sítích s velkým pohybem. Je zde vidět jednorázový nárůst průměrného stupně až na výjimku v podobě S1, kdy tento nárůst probíhal déle než jedno časové okno. Nelze také odpozorovat, že by se v určitém časovém okně stával tento nárůst pravidlem. Všiml jsem si ale toho, že až na výjimku v podobě S1 tyto nárůsty už nepřichází po časovém okně 15. Pokud tedy budu uvažovat o tom, že tyto nárůsty stupně indikují velký pohyb ceny Bitcoinu, pak se cena Bitcoinu razantně mění v začátku a hlavně v průběhu formování svíčky. Čím víc se blíží zavírání svíčky, tím méně nárůstů je z dat pozorováno a tím pádem se cena už moc nehýbe.

U malých pohybů se tento jev vyskytuje také, ale nedochází k tak razantnímu nárůstu kromě výjimky v podobě S1. U dvou sítí s malým pohybem podle Tabulek 34 a 35 dokonce nedošlo k žádnému nárůstu v rámci všech 20 oken. To lze vidět na Obrázku 9. Pokud k určitému nárůstu dojde, u malých pohybů tato hodnota v několika případech vydržela přes více časových oken.



Obrázek 9: Průběh průměrného stupně uzlů u malých pohybů.



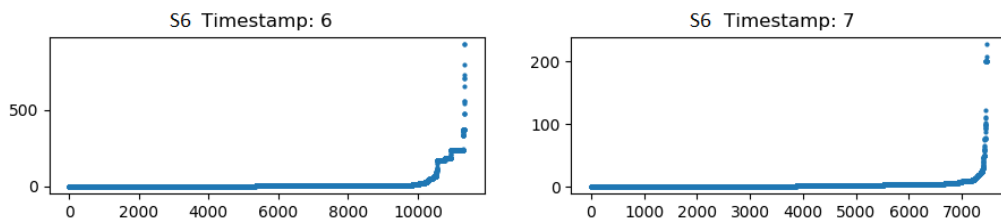
Obrázek 10: Distribuce stupně v jednotlivých časových oknech u velkých pohybů.

V souvislosti s těmito nárůsty stupně jsem se rozhodl analyzovat, zda za těmito nárůsty stojí uzly v řádech jedinců, či větších skupin. Na Obrázku 10 je zachycena část analýzy stupňů u velkého pohybu, konkrétněji u sítě S6. Jednotlivé grafy v obrázku zobrazují distribuci stupňů pro jednotlivá časová okna. Graf vlevo zachycuje časové okno s nadprůměrným nárůstem průměrného stupně a graf vpravo ukazuje časové okno, kdy je průměrný stupeň v klidové hodnotě. Osa x pak popisuje pořadové číslo uzlu, kdežto osa y popisuje uzel daného stupně. Stejný popis grafu patří i k Obrázku 11. Lze vidět odlišnost v tom, že v grafu vlevo je větší skupina uzlů, která má vyšší stupeň, než je tomu u grafu s klidovou hodnotou.

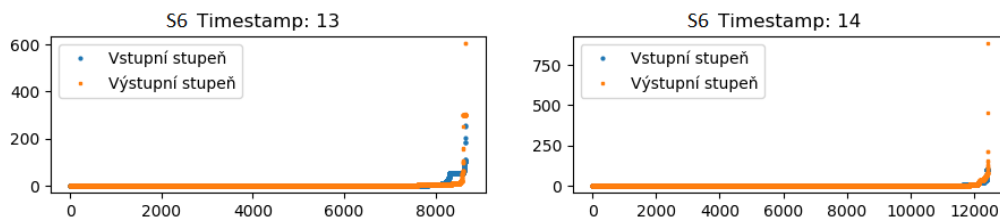
Z tohoto obrázku lze pozorovat rozdíl distribucí v momentě kdy došlo k nárůstu a kdy ne. Pokud k nárůstu nedošlo, křivka vypadá jako klasický power-law graf, kdy většina stupňů má nulovou, či velice malou hodnotu stupně. V síti pak existuje několik uzlů, jejichž stupeň pak výrazně převyšuje zbytek sítě.

Pokud však nastal nárůst průměrného stupně, lze pozorovat, že ve většině případů dochází k nárůstu stupně v křivce dříve. To dokazuje fakt, že existuje podstatně více uzlů, jejichž stupeň převyšuje zbytek sítě. To lze například pozorovat na Obrázku 10 vlevo. Vyskytují se však i případy, kdy má tento nárůst na svědomí jedinec, nicméně tuto situaci jsem pozoroval méně





Obrázek 11: Distribuce stupně v jednotlivých časových oknech u malých pohybů.



Obrázek 12: Distribuce vstupního a výstupního stupně u velkých pohybů.

častěji, než skupinový nárůst stupně.

Pro doplnění na Obrázku 11 je varianta sítě S6 ve varianě malého pohybu. I zde lze pozorovat stejný fenomén jako u příkladu s velkým pohybem.

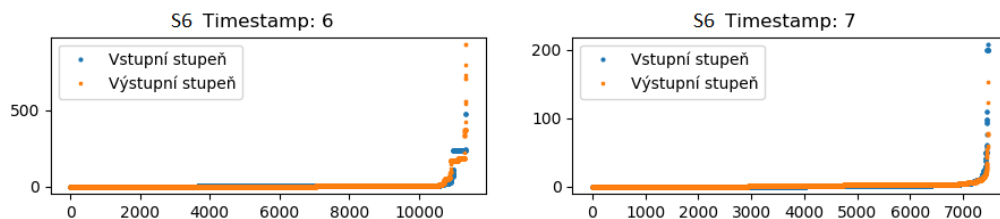
V tomto typu analýzy jsem pak šel ještě o něco hlouběji a rozdělil jsem stupně na vstupní a výstupní a pokoušel jsem se zjistit, zda na tento nárůst mají vliv oba typy stupně, či nikoliv. Na Obrázku 12 je opět část sítě S6 ve variantě s velkým pohybem. Osa x znázorňuje pořadové číslo uzlu a osa y popisuje stupeň daného uzlu. Graf vlevo znázorňuje situaci při vysokém nárůstu průměrného stupně. Graf vpravo ukazuje situaci při průměrném stupni v klidových hodnotách. Stejný popis patří i k Obrázku 13.

Graf nyní zachycuje stejná časová okna jako předtím, ale jedno okno grafu obsahuje distribuci vstupního i výstupního stupně. Zde ve většině případů mají na nárůstu průměrného stupně stejný podíl vstupní i výstupní stupeň. V grafu vlevo lze ale vidět vlastnost, která je vidět ve více případech s velkým pohybem a sice, že výstupní stupeň má strmější nárůst distribuce. Svědčilo by to o tom, že větší vstupní stupeň uzlů se projevuje u větší části sítě než zvýšený výstupní stupeň.

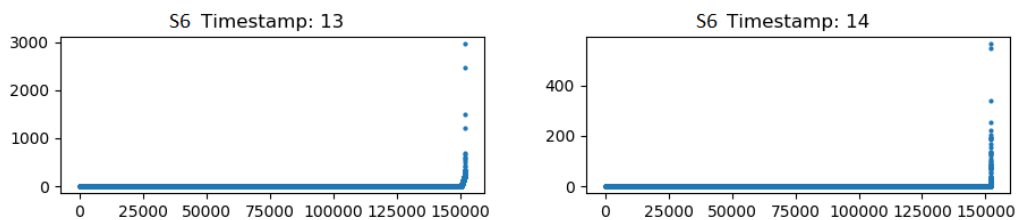
Pro doplnění na Obrázku 13 je část sítě S6 ve variantě s malým pohybem. Zde ve všech případech kdy došlo k zvýšení průměrného stupně mají oba typy stupně stejný podíl na tomto růstu.

### 5.3.2 Analýza betweenness centrality u temporálních sítí

Dalším logickým krokem byla analýza betweenness centrality a to z důvodu toho, zda se prokáže podobná závislost pohybu ceny na betweenness centralitě jako u statických sítí. Analýzu této charakteristiky jsem pojal stejným způsobem jako analýzu stupně u temporálních sítí a to tak,



Obrázek 13: Distribuce vstupního a výstupního stupně u malých pohybů.

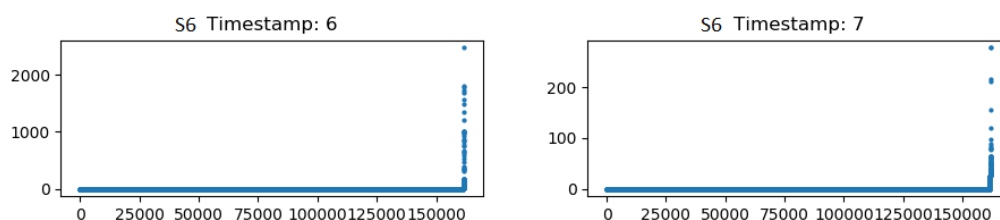


Obrázek 14: Distribuce betweenness u velkých pohybů.

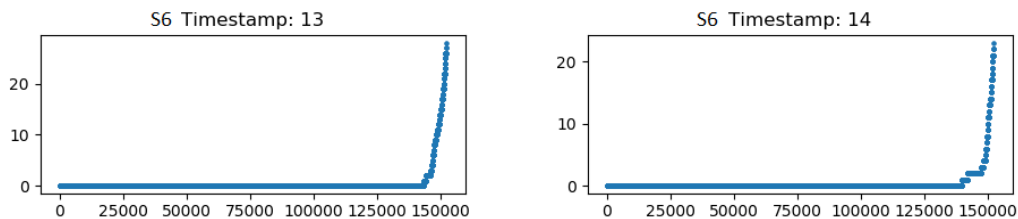
že jsem sestrojil distribuci betweenness centrality u všech časových oken. Na Obrázku 14 je opět část sítě S6 ve variantě s velkým pohybem. Opět graf nalevo ukazuje situaci s vyšší průměrnou hodnotou stupně a graf vpravo znázorňuje situaci s průměrným stupněm v klidových hodnotách. Osa x popisuje pořadové číslo uzlu a osa y znázorňuje betweenness centralitu daného uzlu. Stejný popis platí i pro Obrázek 15.

V tomto případě jsem však nenašel žádnou zvláštnost, která by dokázala oddělit situace s velkým nárůstem stupně od situací, kdy se v podstatě nic neděje. Jde vidět, že veškeré distribuce víceméně vypadají stejně.

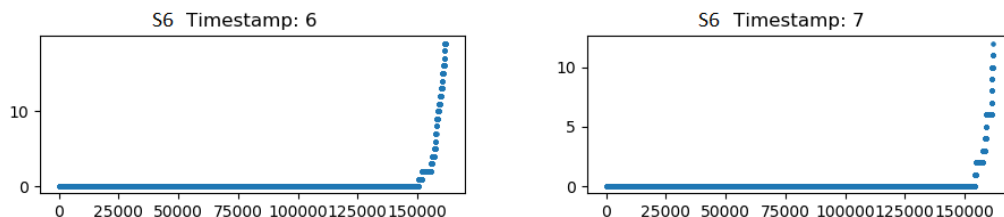
Na Obrázku 15 je část sítě S6 ve variantě s malým pohybem. Ani zde se nedá vyzorovat žádný rozdíl mezi situacemi kdy se nic neděje a situacemi kdy dochází ke zvýšení průměrného stupně. Pokud tento obrázek porovnáme s grafem na Obrázku 14, tak nelze ani určit způsob jak pomocí této charakteristiky určit, zda se jedná o velký či malý pohyb.



Obrázek 15: Distribuce betweenness u malých pohybů.



Obrázek 16: Distribuce excentricity u velkých pohybů.



Obrázek 17: Distribuce excentricity u malých pohybů.

### 5.3.3 Analýza excentricity

Poslední věcí, kterou jsem u temporálních sítí zkoumal byl excentricita vrcholů v síti. Hodnota excentricity vrcholu v síti odpovídá nejkratší možné cestě mezi konkrétním vrcholem a jeho nejvzdálenějším vrcholem. Důvodem této analýzy byly nepřesvědčivé výsledky analýzy betweenness centrality a chtěl jsem si ověřit, že u temporálních sítí charakteristiky nejkratších cest neindikují žádnou zvláštnost, podle které by se dala určit přítomnost velkého pohybu ceny Bitcoinu.

Na Obrázku 16 je část excentricity sítě S6 ve variantě s velkým pohybem. Osa x popisuje pořadové číslo uzlu. Osa y pak popisuje excentricitu daného uzlu. Graf vlevo znázorňuje situaci při vysokém nárůstu průměrného stupně. Graf vpravo ukazuje situaci při průměrném stupni v klidových hodnotách. Stejný popis patří i k Obrázku 17. Bohužel ani tato metrika neukazuje žádné odchylky v situaci, kdy došlo k navýšení stupně v síti. Můžeme však pozorovat, že i v temporálních sítích jsou si i nejvzdálenější vrcholy poměrně blízké.

Opět pro doplnění na Obrázku 17 je část distribuce excentricity v síti S6 ve variantě s malým pohybem. Ani zde se neukazuje žádná odchylka mezi jednotlivými časovými okny ani mezi variantou s velkým a malým pohybem.

## 5.4 Analýza adres

Ze statické analýzy, konkrétněji z analýzy betweenness centrality a z analýzy distribuce stupňů v síti, vyplynula informace, že se v síti tvoří centrální uzly, skrze které vede velké množství nejkratších cest, a které spojují uzly do větších komponent. Rozhodl jsem se proto podívat blíže na tyto HUBy a zkusit propojit jednotlivé adresy centrálních uzlů s určitými entitami, jako jsou například kryptoburzy. K dohledávání jsem použil službu [27]. Zkoušel jsem také dohledat adresy skrze internetové vyhledávače.

#### 5.4.1 Unikátní adresy v sítích

Nejdříve jsem zkoušel zjistit, zda v sítích s velkým pohybem existují centrální uzly, které se v sítích s malým pohybem nevyskytují. Abych byl toto schopný provést, prošel jsem všechny sítě s velkým i malým pohybem a vybral jsem z každé z nich 5 uzlů s největším stupněm.

V tabulce 27 je část unikátních adres z velkých pohybů. Je jich celkem 55, z čehož bylo identifikováno 12. Z tabulky lze vidět, že se v ní objevují adresy, které se vyskytují skoro ve všech sítích mezi uzly s největším stupněm. Tyto adresy odpovídají kryptoburzám Binance a Huobi.

Zarazilo mě, kolik adres je spojeno s nějakým podvodem, či rovnou kriminální aktivitou. Adresy, které byly spojeny s webovými adresami Investmentdouble.online (již nefunkční), Bitbay.mtro.club, Bitcompany.io (již nefunkční) byly několikrát nahlášeny jako podvodné služby, kam uživatelé naposílali jejich Bitcoinů s vidinou jejich zdvojnásobení. Ve skutečnosti však poslané Bitcoinů už nikdy neviděli. Jedna z adres byla nahlášena ve spojení s phishingem a jedna z adres byla dokonce vytrasována k ransomwaru, kam uživatelé měli poslat Bitcoinů výměnou za klíč k odšifrování obsahu jejich disku, který byl předtím tímto ransomwarem zašifrován. Jestli však klíče fungovaly, jsem nedokázal dohledat.

To že se tyto adresy dostaly mezi 5 uzlů s největším stupněm (některé dokonce několikrát), může indikovat několik skutečností. Jednou z nich může být množství podvedených lidí. Aby se tyto adresy dostaly do 5 uzlů s největším stupněm, musely to být stovky lidí, kteří jim uvěřili. Druhou možností proč mají tyto adresy hodně transakcí je používání nezákonně nabytých prostředků k financování mnoha dalších věcí.

Následovala analýza adres v malých pohybech. Ta je vidět v Tabulce 28. V tomto případě se vyskytlo 53 unikátních adres, z nichž bylo 11 dohledáno. I zde se opakují adresy odpovídající kryptoburzám Binance a Huobi a opět mají četné zastoupení skrze více sítí. Podvodné adresy se vyskytují i zde, ale v menším počtu (5 podvodných adres oproti 9 u velkých pohybů).

V této části jsem zjistil, že počet unikátních adres centrálních uzlů se u sítí s velkými pohyby neliší od počtu u sítí s malými pohyby. Nepodařilo se ani najít adresu, která by se často vyskytovala při velkých pohybech a u malých pohybů by se neprojevovala. Našly se však centrální uzly, které se vyskytují často v obou typech pohybů a to jsou uzly patřící velkým kryptoburzám. Tato informace poukazuje, že nedochází k ovlivňování ceny Bitcoinu samotnými burzami. Pokud by toto ovlivňování probíhalo, muselo by se jednat o sofistikovanější způsob zahrnující mnoho adres, které by se neopakovaly, nebo by se opakovaly velmi zřídka.

#### 5.4.2 Adresy patřící ke 100 nejbohatším bitcoinovým adresám

V případě velkých i malých pohybů se objevilo několik adres, které patří mezi 100 nejbohatších bitcoinových adres. V obou případech to bylo 7 adres, přičemž se 3 adresy z tohoto seznamu objevují u velkých i malých pohybů a jedna z těchto tří adres byla často nahlašována jako podvodná adresa.

Adresa	Počet výskytů	Subjekt
1NDyJtNTjmwk5xPNhJgAMu4HDHigtobu1s	18	Binance
1HckjUpRGerrRAAtFaaCAUaGjsPx9oYmLaZ	16	Huobi
3NrTf9Q2amgZLkESJzvCF5enRdjwQNwFvb	4	?
3AQ4kUjQaDjCjmDh2ojKEHjUKTSi52UUqD	3	Investmentdouble.online
3JXRVxhRk2o9f4w3cQchBLwUeegJBj6BEp	2	Investmentdouble.online
1GyKjyyBo67ZG5tXF3EniF8j8ohNQddYek	2	?
15krWJTArivNmXgZZzPENv3ohh2AwdQDgH	2	?
3G1nNTTyrpZBwyEiG6U3bJvZdu9sW3rbUz	1	Bitcompany.io
1Q7PQaWurNiBuzdjxwR7njktWB9e92wqW	1	Podvodná
14AM3T26CRqC2rM8LQ1SE5HuUyJacSk4Uy	1	Huobi
35hK24tcLEWcgNA4JxpvbkNkoAcDGqQPSP	1	Huobi cold wallet
1MFgcyJ7ZNSknBTBRaih6zWDE6V1A64tRY	1	PlusToken investment
1G47mSr3oANXMafVrR8UC4pzV7FEAzo3r9	1	Bitbay.mtro.club
3EEJfjZURxShNr2AoJtbfcvCB749yzP7LP	1	e-mailový podvod
38f8RHFQ8v6avZqCmaYTga5bTYiuhoM6fh	1	ransomware, vydírání
bc1qa24tsgchvuxsaccp8vrnkfd85hrpafg20kmjw	1	Wasabi wallet

Tabulka 27: Tabulka unikátních adres u velkých pohybů

Adresa	Počet výskytů	Subjekt
1NDyJtNTjmwk5xPNhJgAMu4HDHigtobu1s	19	Binance
1HckjUpRGerrRAAtFaaCAUaGjsPx9oYmLaZ	14	Huobi
3JF8UKBhhfGQ5w1CpnSQhpzi4f8F3dg3H9	4	Podvod
17ac9tXHxu1nxdLgLu9WYk7vR8ggFN5GkH	3	Podvod
3AQ4kUjQaDjCjmDh2ojKEHjUKTSi52UUqD	2	Investmentdouble.online
1GX28yLjVWux7ws4UQ9FB4MnLH4UKTPK2z	2	Mining pool
3JXRVxhRk2o9f4w3cQchBLwUeegJBj6BEp	2	Investmentdouble.online
bc1q80yv24hnlpgyh5kdnppdZg6w3yxhkrduqs3ty8	2	?
3PiMUCgxZUYRPJ2VATyhYbePXxRTHBjAtr	2	?
38ENmTr2AD1avJrmmi9iM7PfS6nZVmuMKf	2	?
12f8twoiaNQWiMBpQCqCz11PgnBV1pzS8g	2	Huobi
19QejPzSKEiVro33rX7Qp4WSPcuZCvgB6A	2	?
1qao1XoK59f8pp5e8cC1bXHzQnw4CH5t5	2	?
3EEJfjZURxShNr2AoJtbfcvCB749yzP7LP	2	e-mail podvod
1Hz96kJKF2HLPgy15JWLB5m9qGNxvt8tHJ	1	Mining pool
1Q2yHXMPHwRLaQf5XrH3kF7hDNtpr2bJ3d	1	Doubler-Bitcoin.com
3JX5A5eWjVR8BgtBgxJYNTpknAc3gEbsz2	2	?

Tabulka 28: Tabulka unikátních adres u malých pohybů

U velkých pohybů se jedná o tyto adresy:

- 1HckjUpRGerrRAAtFaaCAUaGjsPx9oYmLaZ
- 1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s
- 3JXRvXhrk2o9f4w3cQchBLwUeegJBj6BEp
- 3NrTf9Q2amgZLkESJzvCF5enRdjwQNwFvb
- 35hK24tcLEWcgNA4JxpvbkNkoAcDGqQPSP
- 1G47mSr3oANXMafVrR8UC4pzV7FEAzo3r9
- 3JRgbZ6d2pMR3p37uRYW3VNCvDEq12kk6E

Právě třetí adresa je spojena s podvodným zdvojnásobováním Bitcoinů. Podstatná část těchto adres pak tvoří adresy patřící kryptoburzám, které uchovávají bitcoiny zaregistrovaných uživatelů, viz Tabulka 27.

U malých pohybů jsou to pak následující adresy:

- 1HckjUpRGerrRAAtFaaCAUaGjsPx9oYmLaZ
- 1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s
- 3JXRvXhrk2o9f4w3cQchBLwUeegJBj6BEp
- 3K1PN3MGtXxmUAKACNwudxx8X1iv96AXGJ
- 17ac9tXHxu1nxdLgLu9WYk7vR8ggFN5GkH
- 1Q2yHXMPHWRLaQf5XrH3kF7hDNtpr2bJ3d
- 36gvNqMu8TUUMgq3hAoo8HFndVRozqp5fA

V případě malých pohybů se mezi těmito adresy vyskytují hned dvě podvodné adresy. Třetí adresa v tomto seznamu je i v seznamu nejbohatších adres u velkých pohybů. Druhá tato podvodná adresa je druhá od konce a jedná se také o službu zdvojnásobování vkladů.

Celkový přehled identifikovaných adres u velkých adres je vidět na Obrázku 18, u malých adres je to pak Obrázek 19.

Z jednotlivých výsečových grafů lze vidět, že většinu unikátních centrálních adres se nepodařilo identifikovat a spojit s příslušným subjektem. Pokud se to však podařilo, tak v obou případech mají největší zastoupení podvodné adresy, které souvisí s nekalými praktikami. Druhým nejzastoupenějším odvětvím jsou burzy. U malých pohybů se pak vyskytly dva případy adres spojované s těžebními službami.



Obrázek 18: Zastoupení identifikovaných unikátních adres u velkých pohybů



Obrázek 19: Zastoupení identifikovaných unikátních adres u malých pohybů

Den v týdnu	Počet velkých pohybů
Pondělí	1
Úterý	3
Středa	6
Čtvrtek	1
Pátek	4
Sobota	4
Neděle	1

Tabulka 29: Tabulka počtu velkých pohybů v závislosti na dni v týdnu

## 5.5 Analýza výskytu velkých pohybů

Další zajímavostí na kterou jsem narazil byla analýza dnů, ve kterých se vyskytují velké pohyby. Jelikož jsem se při výběru mé datové sady díval pouze na to, jak moc cena Bitcoinu vyskočila nebo poklesla, tak jsem zkoušel zjistit, jestli existuje nějaké pravidlo, kdy se častěji vyskytovaly velké pohyby čistě podle dne v týdnu, nebo podle dne v měsíci.

Nejprve jsem analyzoval den v týdnu. Ten je v Tabulce 29. Z tabulky lze vidět, že zastoupení má každý den. Nejčastěji se velké pohyby vyskytovaly ve středu a to až ve 30% případů. Dále má výrazné zastoupení dvojice dnů pátek, sobota, která dohromady tvoří 40% případů výskytu velkého pohybu.

Z této tabulky lze usoudit, že největší šance na výskyt velkého pohybu ceny Bitcoinu lze očekávat buď uprostřed týdne, a nebo pak ke konci týdne, kde je pravděpodobnost ještě vyšší.

Následovala analýza dne v měsíci. Ten je zachycen v Tabulce 30. Z tabulky na první pohled jde vidět, že se pravděpodobnost výskytu velkého pohybu zvyšuje s koncem měsíce. Podle této tabulky je šance na velký pohyb po 22. dni v měsíci je 50%, přičemž dny 25. a 26. tvoří 25% všech výskytů velkých pohybů v mé datové sadě.

Shrnutím této části je, že podle roku 2019 se pravděpodobnost velkého pohybu zvyšuje s blížícím se koncem měsíce a nejčastěji na přelomu začátku a prostředku týdne (úterý, středa) nebo koncem týdne (pátek, sobota). Jestli se tento výskyt dá zobecnit, bylo by potřeba provést stejnou analýzu na datech posbíraných z více let cenových dat Bitcoinu.



Den v měsíci	Počet velkých pohybů
2	1
4	1
6	2
10	2
17	1
18	1
22	2
23	1
24	1
25	2
26	3
28	1

Tabulka 30: Tabulka počtu velkých pohybů v závislosti na dni v měsíci

## 6 Pokračování analýzy

Mnou provedená analýza má velký potenciál k vylepšení. Jednou z možností vylepšení a zpřesnění výsledků je nasbírat větší počet dat a to i z různých let Bitcoinu. Mělo by se však jednat o data z fáze, kdy už byl Bitcoin více používán, jelikož data z počátku Bitcoinu by pravděpodobně zkreslovaly naměřené výsledky.

Dalším způsobem jak zkvalitnit tuto analýzu je zahrnout do sítí kromě samotných transakcí i daný objem Bitcoinů, který se v dané transakci poslal a to například v podobě ohodnocení samotných hran. Jsem přesvědčen o tom, že pomocí tohoto faktoru by se dalo oddělit velké pohyby od těch malých, avšak nenapadla mě žádná vhodná metoda, jak tuto vlastnost do sítí zahrnout.

## 7 Závěr

Cílem této práce bylo odhalit rozdíl vlastností sítí s velkým resp. malým pohybem ceny Bitcoinu a predikovat pomocí těchto sítí případný velký pohyb v ceně Bitcoinu. Pro vyřešení tohoto problému byly použity nástroje pro vytvoření a analýzy komplexních sítí a to jak statických tak dynamických. Konkrétně to byly nástroje Gephi, Pajek, společně s python knihovnou Networkx. Statistická data byla spočítána pomocí jazyka R. Pro stažení dat Bitcoinu byl použit jazyk python společně s programem Bitcoin Core, který slouží jako Bitcoinový klient.

Závěrem mé práce je zjištění, že se velké pohyby ceny Bitcoinu neprojevují přímo v počtu transakcí nebo v počtu adres, které se transakcí účastní. Projevují se nejvíce v tom, že se vyskytují adresy, přes které vede větší počet transakcí než je tomu u malých pohybů. Často se stává, že takovéto adresy jsou spojovány s podvodnou činností z minulosti, nebo se jedná o adresy patřící burzám.

Experimentální část odhalila rozdíl mezi velkými a malými pohyby ve statických sítích pouze u betweenness centrality, kdy se u velkých pohybů vyskytuje vyšší betweenness centralita než u pohybů malých. U temporálních sítí se rozdíl objevil ve vyšším průměrném stupni uzlů u velkých pohybů. Následná detailní analýza stupně v temporálních sítích odhalila, že se nejedná o nárůst stupně mezi jednotlivci, ale nárůst má na svědomí větší skupina uzlů v Bitcoinové síti, tudíž se nejedná o umělou manipulaci ceny mezi jednotlivci.

Pokud se tedy nejedná o manipulaci s cenou ze strany burz, tak se jedná o situace, kdy se velké množství subjektů rozhodne manipulovat s jejich vlastními Bitcoinů a tím se dá do pohybu i cena Bitcoinu. Takové manipulace zahrnují buď posílání Bitcoinů v rámci nákupu či prodeje komunit a nebo se jedná o nákup či prodej samotných Bitcoinů za reálné peněžní prostředky.

Dalším faktem, který jsem odhalil byl ten, že pravděpodobnost velkého pohybu se zvyšuje s rostoucím dnem v měsíci. Velký pohyb je také nejpravděpodobnější ke konci týdne. Bude určitě zajímavé sledovat, jestli se tento fenomén potvrdí také v roce 2020.

## Literatura

1. LIU, Keshi; WENG, Tongfeng; GU, Changgui; YANG, Huijie. Visibility graph analysis of Bitcoin price series. *Physica A: Statistical Mechanics and its Applications*. 2020, roč. 538, s. 122952. ISSN 0378-4371. Dostupné z DOI: <https://doi.org/10.1016/j.physa.2019.122952>.
2. ZOU, Yong; SMALL, Michael; LIU, Zonghua; KURTHS, Jürgen. Complex network approach to characterize the statistical features of the sunspot series. *New Journal of Physics*. 2014-01, roč. 16, č. 1, s. 013051. Dostupné z DOI: [10.1088/1367-2630/16/1/013051](https://doi.org/10.1088/1367-2630/16/1/013051).
3. MAESA, D. D. F.; MARINO, A.; RICCI, L. Uncovering the Bitcoin Blockchain: An Analysis of the Full Users Graph. In: *2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*. 2016-10, s. 537–546. Dostupné z DOI: [10.1109/DSAA.2016.52](https://doi.org/10.1109/DSAA.2016.52).
4. BACKSTROM, Lars; BOLDI, Paolo; ROSA, Marco; UGANDER, Johan; VIGNA, Sebastiano. Four Degrees of Separation. *CoRR*. 2011, roč. abs/1111.4570. Dostupné z arXiv: [1111.4570](https://arxiv.org/abs/1111.4570).
5. MAESA, Damiano; MARINO, Andrea; RICCI, Laura. Data-driven analysis of Bitcoin properties: exploiting the users graph. *International Journal of Data Science and Analytics*. 2017-09. Dostupné z DOI: [10.1007/s41060-017-0074-x](https://doi.org/10.1007/s41060-017-0074-x).
6. MAESA, Damiano; MARINO, Andrea; RICCI, Laura. An analysis of the Bitcoin users graph: inferring unusual behaviours. In: 2017-11, sv. 693, s. 749–760. ISBN 978-3-319-50900-6. Dostupné z DOI: [10.1007/978-3-319-50901-3\\_59](https://doi.org/10.1007/978-3-319-50901-3_59).
7. *Pseudo-spam transakce* [online] [cit. 2019-02-05]. Dostupné z: <https://www.blockchain.com/btc/tx/35dead89c059e846e2013a06a70cd84a7ba0f80da7741c283d6efd573e0a7319>.
8. MAESA, Damiano; MARINO, Andrea; RICCI, Laura. The bow tie structure of the Bitcoin users graph. *Applied Network Science*. 2019-12, roč. 4. Dostupné z DOI: [10.1007/s41109-019-0163-y](https://doi.org/10.1007/s41109-019-0163-y).
9. RAGHAVAN, Prabhakar. Graph Structure of the Web: A Survey. In: GONNET, Gaston H.; VIOLA, Alfredo (ed.). *LATIN 2000: Theoretical Informatics*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, s. 123–125. ISBN 978-3-540-46415-0.
10. KONDOR, Dániel; PÓSFAL, Márton; CSABAI, István; VATTAY, Gábor. Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network. *PLOS ONE*. 2014-02, roč. 9, č. 2, s. 1–10. Dostupné z DOI: [10.1371/journal.pone.0086197](https://doi.org/10.1371/journal.pone.0086197).
11. LISCHKE, Matthias; FABIAN, Benjamin. Analyzing the Bitcoin Network: The First Four Years. *Future Internet*. 2016, roč. 8, s. 7.

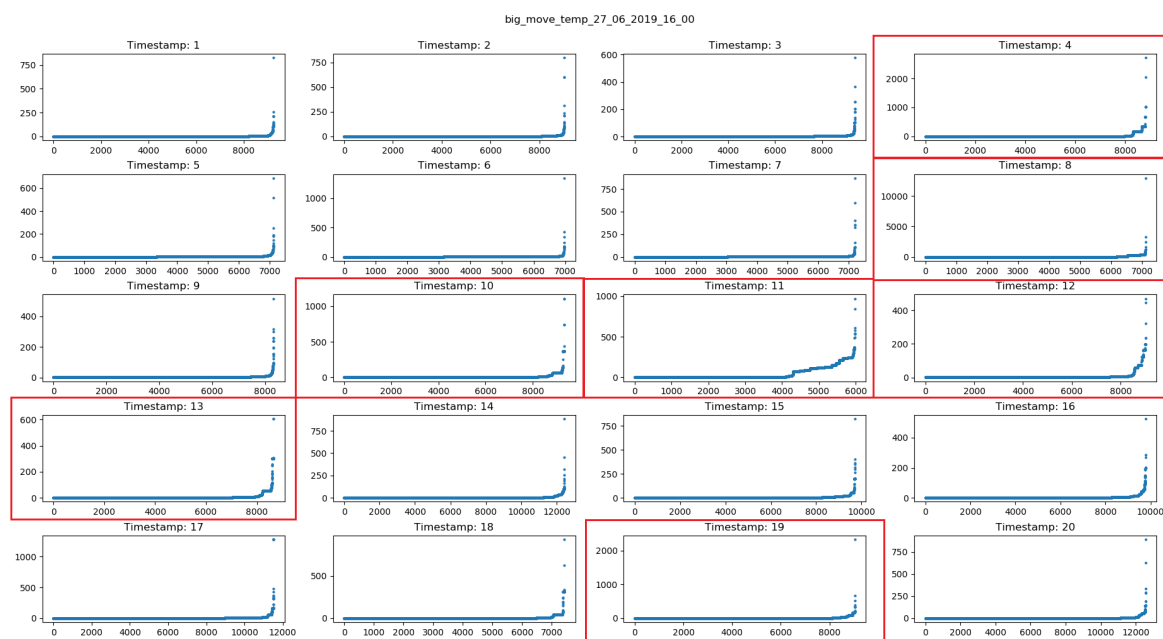
12. LAHMIRI, Salim; BEKIROS, Stelios. Chaos, randomness and multi-fractality in Bitcoin market. *Chaos, Solitons & Fractals*. 2018, roč. 106, s. 28 –34. ISSN 0960-0779. Dostupné z DOI: <https://doi.org/10.1016/j.chaos.2017.11.005>.
13. LIANG, Jiaqi; LI, Linjing; ZENG, Daniel. Evolutionary dynamics of cryptocurrency transaction networks: An empirical study. *PLOS ONE*. 2018-08, roč. 13, č. 8, s. 1–18. Dostupné z DOI: [10.1371/journal.pone.0202202](https://doi.org/10.1371/journal.pone.0202202).
14. NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. *Cryptography Mailing list at https://metzdowd.com*. 2009-03.
15. Úvod do teorie grafů [online] [cit. 2019-04-20]. Dostupné z: [http://home1.vsb.cz/~kov16/files/uvod\\_do\\_teorie\\_grafu.pdf](http://home1.vsb.cz/~kov16/files/uvod_do_teorie_grafu.pdf).
16. DE NOOY, Wouter; MRVAR, Andrej; BATAGELJ, Vladimir. *Exploratory Social Network Analysis with Pajek*. Cambridge University Press, 2018.
17. COLEMAN, Thomas F.; MORÉ, Jorge J. Estimation of Sparse Jacobian Matrices and Graph Coloring Problems. In: 1983.
18. WATTS, Duncan J; STROGATZ, Steven H. Collective dynamics of ‘small-world’ networks. *nature*. 1998, roč. 393, č. 6684, s. 440.
19. SOHN, Insoo. Small-World and Scale-Free Network Models for IoT Systems. *Mobile Information Systems*. 2017-01, roč. 2017, s. 6752048. ISSN 1574-017X. Dostupné z DOI: [10.1155/2017/6752048](https://doi.org/10.1155/2017/6752048).
20. RAGHAVAN UNNITHAN, Sunil Kumar; KANNAN, Balakrishnan; JATHAVEDAN, Madambi. Betweenness Centrality in Some Classes of Graphs. *International Journal of Combinatorics*. 2014-12, roč. 2014, s. 241723. ISSN 1687-9163. Dostupné z DOI: [10.1155/2014/241723](https://doi.org/10.1155/2014/241723).
21. *Reciprocita hran* [online] [cit. 2019-04-20]. Dostupné z: <https://sites.google.com/site/ucinetsoftware/document/faq/reciprocity--arcordyad>.
22. NEWMAN, M. E. J. Mixing patterns in networks. *Physical Review E*. 2003-02, roč. 67, č. 2. ISSN 1095-3787. Dostupné z DOI: [10.1103/physreve.67.026126](https://doi.org/10.1103/physreve.67.026126).
23. *Typy komplexních sítí* [online] [cit. 2019-04-22]. Dostupné z: [http://www.cs.vsb.cz/ochodkova/courses/MADI/madi\\_03.pdf](http://www.cs.vsb.cz/ochodkova/courses/MADI/madi_03.pdf).
24. *Bitcoin API* [online] [cit. 2019-04-10]. Dostupné z: <https://www.blockchain.com>.
25. *Bitcoin API* [online] [cit. 2019-04-10]. Dostupné z: <https://www.smartbit.com.au>.
26. SCHOLTES, Ingo; WIDER, Nicolas; GARAS, Antonios. Higher-order aggregate networks in the analysis of temporal networks: path structures and centralities. *The European Physical Journal B*. 2016-03, roč. 89, č. 3. ISSN 1434-6036. Dostupné z DOI: [10.1140/epjb/e2016-60663-0](https://doi.org/10.1140/epjb/e2016-60663-0).

27. *Služba pro dohledání subjektů* [online] [cit. 2019-04-10]. Dostupné z: <https://bitcoinwhoswho.com>.

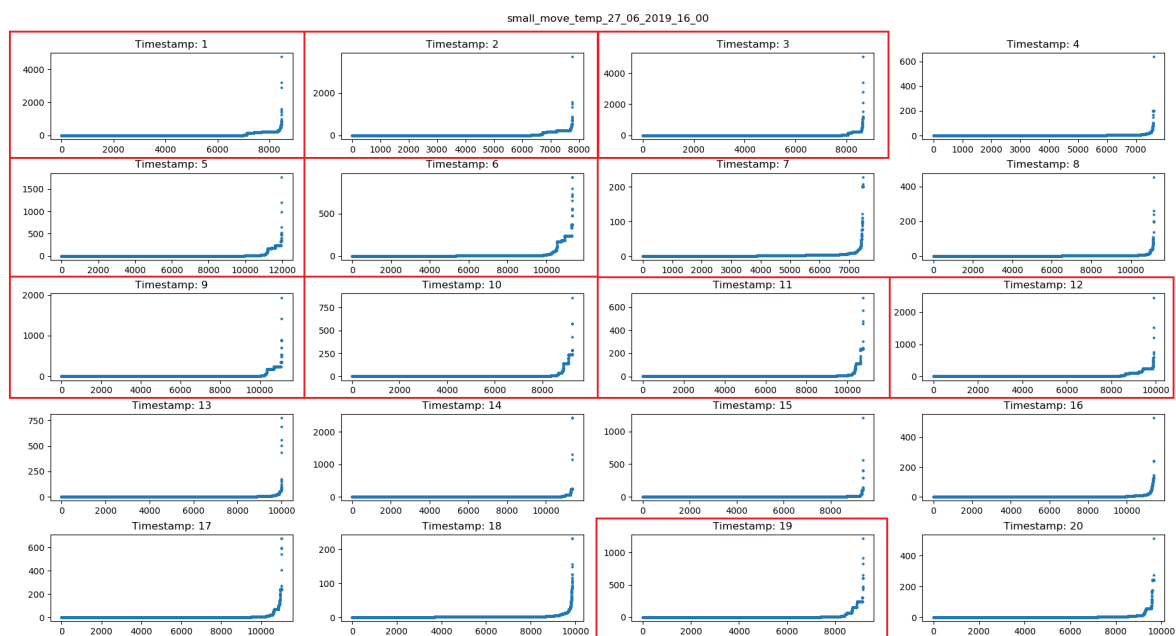
## A Velké obrázky a tabulky

U následujících obrázků červený rámeček znázorňuje časové okno, kdy došlo k nárůstu průměrného stupně nad jeho klidovou hodnotu. Důvodem tohoto označení je nalezení odlišných průběhů dat v momentě kdy došlo k nárůstu průměrného stupně a kdy k takovému nárůstu nedošlo.

Následující grafy mají společnou osu x, která popisuje pořadové číslo uzlu. U Obrázků 20 až 23 osa y zachycuje stupeň uzlu. Osa y u Obrázků 24 a 25 popisuje betweenness centralitu a u Obrázků 26 a 27 je na ose y excentricita daného uzlu.

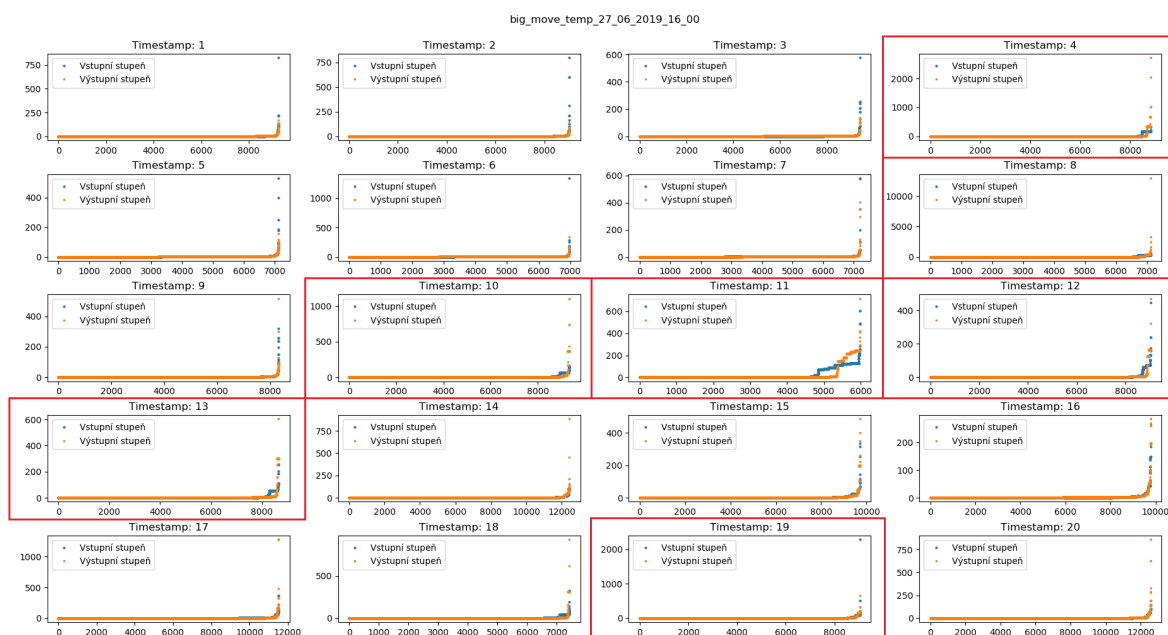


Obrázek 20: Distribuce stupně v jednotlivých časových oknech u velkých pohybů.

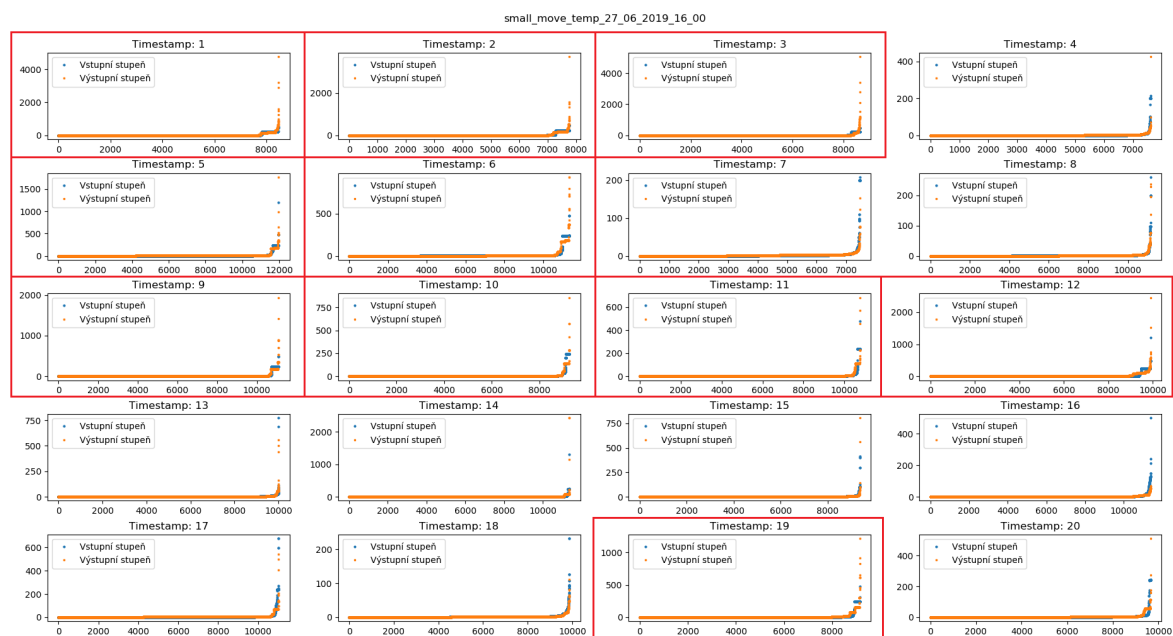


Obrázek 21: Dsitríbuce stupně v jednotlivých časových oknech u malých pohybů.

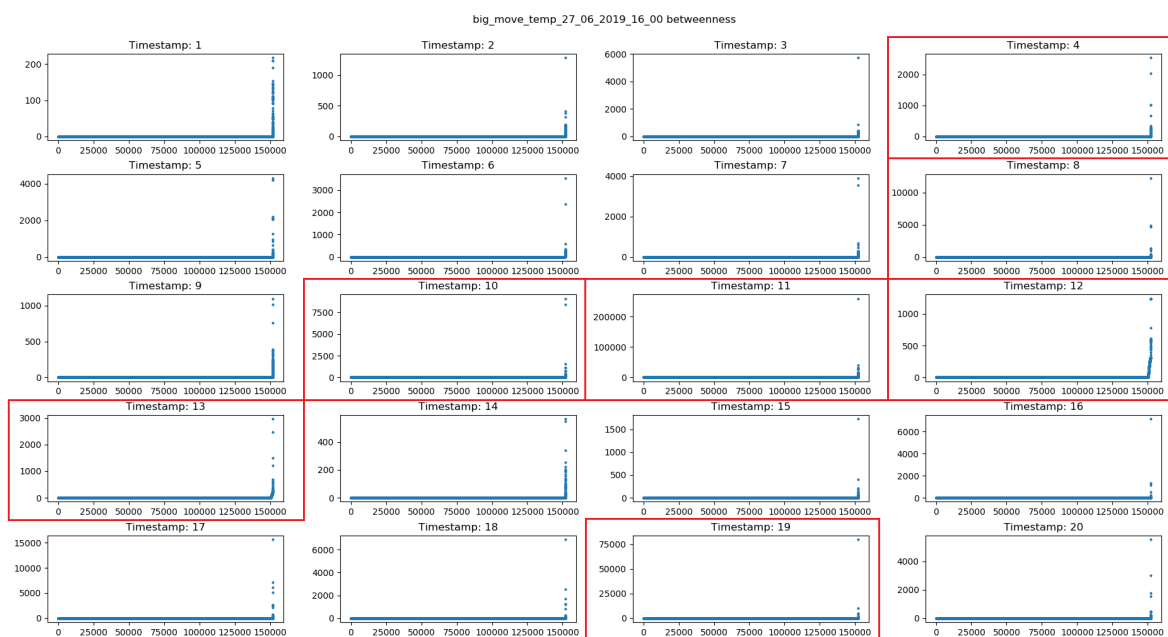




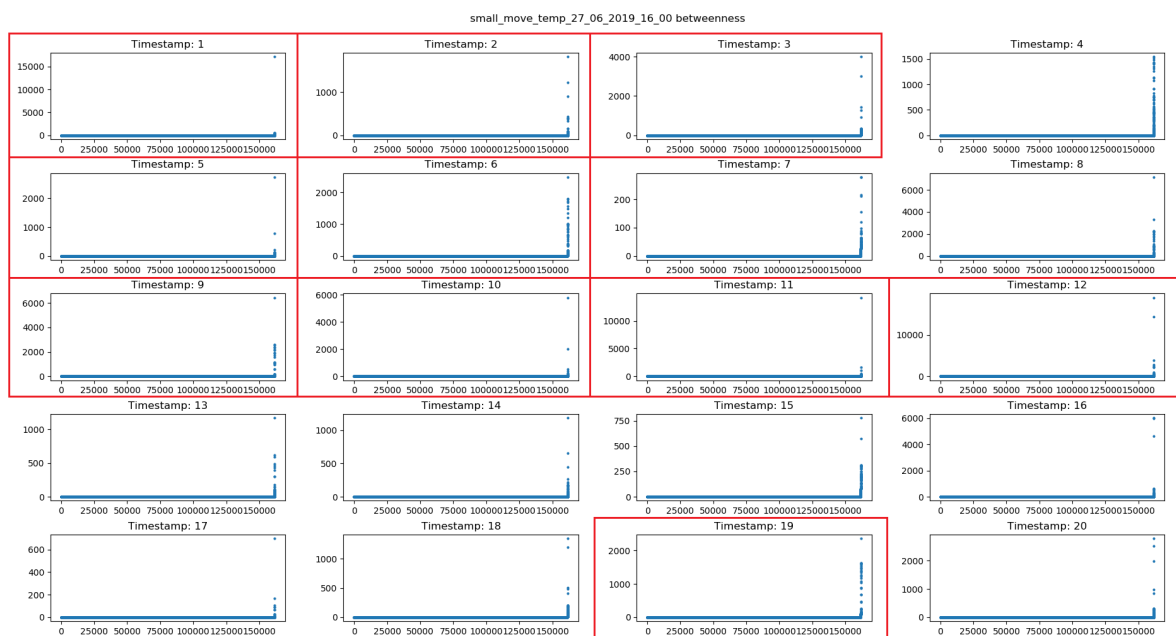
Obrázek 22: Distribuce vstupního a výstupního stupně u velkých pohybů.



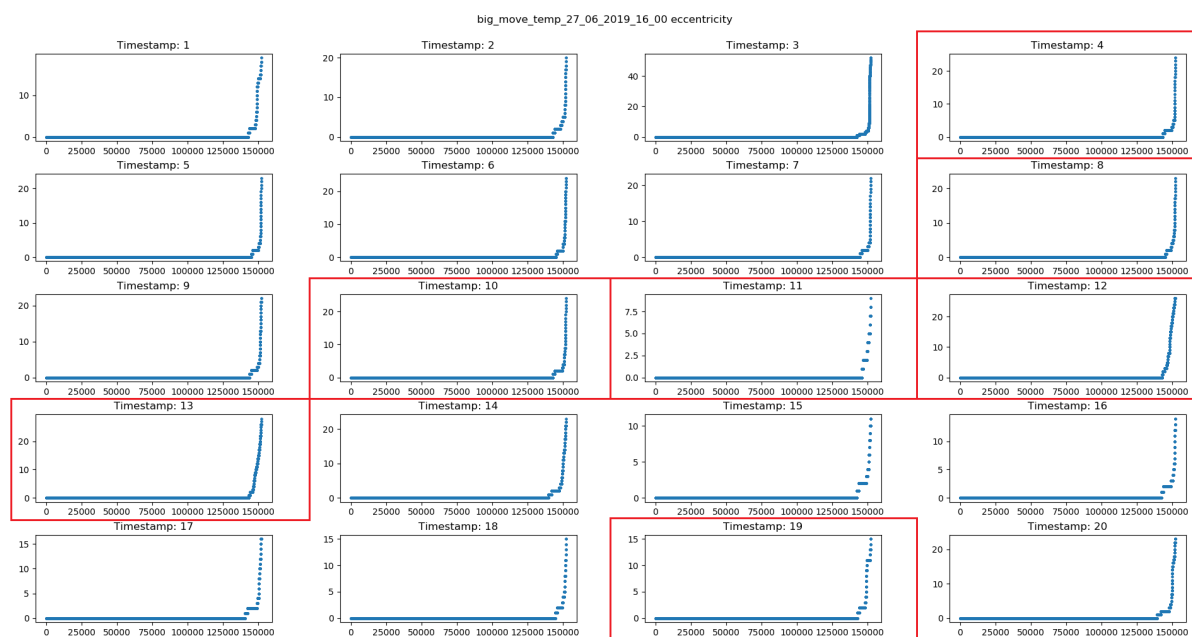
Obrázek 23: Distribuce vstupního a výstupního stupně u malých pohybů.



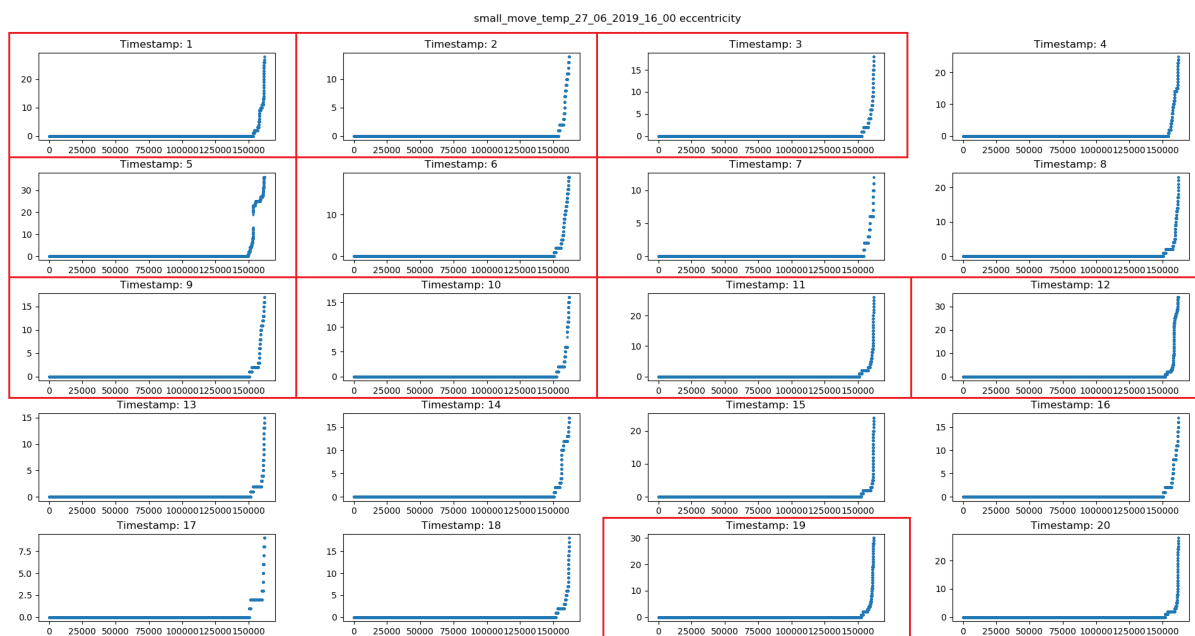
Obrázek 24: Distribuce betweenness u velkých pohybů.



Obrázek 25: Distribuce betweenness u malých pohybů.



Obrázek 26: Distribuce excentricity u velkých pohybů.



Obrázek 27: Distribuce excentricity u malých pohybů.

Časové okno	S1 VP	S1 MP	S2 VP	S2 MP	S3 VP	S3 MP	S4 VP	S4 MP
1	8185	8744	6147	10549	7080	9170	8911	10810
2	9325	2936	10281	9891	6870	9553	9892	8202
3	12169	8035	11434	9769	411	9323	10592	6820
4	8577	3273	10072	10485	684	3161	11369	8351
5	8546	4220	9810	11781	3482	6958	8237	5788
6	5674	6926	11127	9824	9388	10704	9869	5672
7	8451	5049	10792	10614	6782	9790	7235	11703
8	8621	11712	10566	9359	11110	5417	10508	8782
9	8811	11163	10336	7386	3136	11239	9224	6120
10	9315	10368	10454	8115	7533	8218	9588	8864
11	7965	17722	9765	9094	9917	9817	8874	6104
12	9760	11050	11906	7262	10376	6065	8307	5748
13	18243	8740	9313	9960	9575	8129	9460	6131
14	29580	9492	9582	10728	8769	10847	5657	10180
15	8916	9614	10603	5364	9211	10242	5441	6608
16	8777	12077	6795	10324	10232	10521	9793	3894
17	10007	9157	9440	12003	10185	11466	7605	2089
18	10477	8629	5157	9575	10984	10009	7333	6276
19	11554	12081	1383	10848	8837	8678	8239	5094
20	11591	10510	12262	11494	9709	6089	6473	9857
Časové okno	S5 VP	S5 MP	S6 VP	S6 MP	S7 VP	S7 MP	S8 VP	S8 MP
1	7209	6607	9255	8469	8494	7731	213	8575
2	10454	10282	9023	7768	5627	7011	4984	8251
3	9173	431	9415	8642	1943	9288	507	7621
4	5871	6857	8827	7609	9543	7885	3004	5907
5	11235	2629	7121	11975	9950	7048	5521	8051
6	8649	5885	6972	11336	10112	2516	872	5951
7	8301	1550	7207	7470	9537	7057	3239	1977
8	8958	3617	7120	11155	9232	8648	2211	3578
9	9377	6661	8322	11103	11181	10090	2688	1117
10	6445	11614	9334	9259	10116	8939	178	4593
11	9368	4316	5980	10758	8471	7021	10234	4322
12	9678	1499	9025	9908	9454	8451	9487	1545
13	9576	4510	8665	10002	9178	4798	7937	9008
14	3888	11059	12429	11364	9683	8070	8446	8069
15	10474	4953	9712	9375	8083	8491	6040	9451
16	11210	1328	9777	11383	8621	5509	9417	4107
17	9764	3354	11527	11035	6789	5440	9646	1384
18	9634	1276	7427	9863	8122	6537	8611	3088
19	8968	14891	9048	9152	8675	9238	6393	3540
20	8254	4229	1256	9653	8078	9462	7707	5311

Tabulka 31: Tabulka počtu vrcholů v temporálních sítích

Časové okno	S9 VP	S9 MP	S10 VP	S10 MP
1	10544	9155	8855	8751
2	9304	10527	13179	6415
3	10760	10076	10566	10152
4	9812	10539	9214	7107
5	10374	8418	10990	9017
6	10062	6787	10771	9854
7	10163	10323	8339	7259
8	10324	10913	9731	7720
9	9069	10477	10487	5727
10	10292	7663	9985	10951
11	10905	7369	9042	7897
12	10323	9683	11045	6346
13	9709	9672	10631	2481
14	9150	10528	10009	10694
15	10203	1296	10372	9732
16	10960	10975	7063	6051
17	10470	10208	3909	3298
18	10090	8206	10307	11148
19	10896	6823	11584	9053
20	10283	10731	10471	5746

Tabulka 32: Pokračování tabulky počtu vrcholů v temporálních sítích

Časové okno	S1 VP	S1 MP	S2 VP	S2 MP	S3 VP	S3 MP	S4 VP	S4 MP
1	11878	10251	25148	21080	10667	12533	13921	16924
2	11902	10868	17507	17447	13028	16940	36665	12599
3	19164	15847	20942	15307	458	15603	18743	10539
4	13643	12129	14388	14921	763	7146	23159	39956
5	11414	7989	17232	20001	5503	11254	13461	11972
6	12827	13185	18434	16127	56285	23846	278611	8650
7	11221	14876	21257	18193	11385	86530	14442	20822
8	19787	17741	14833	17482	16290	8542	23423	13351
9	14846	16607	15134	9006	5681	16095	22546	9331
10	32700	14829	19262	10737	12017	14213	15535	35233
11	15848	36102	12002	16246	18255	14757	26941	12697
12	15435	58684	62429	12780	15712	13186	25408	7757
13	94272	3044661	16414	16568	16669	13209	25287	10506
14	29580	124913	16729	14122	24739	24715	14557	18933
15	131574	355253	27658	9529	14747	18493	10177	9248
16	85587	160691	21027	23524	15934	15607	22244	8626
17	379199	172640	14988	17581	15068	15416	13074	3985
18	554752	5584	7754	14151	19769	26824	14923	10632
19	435989	204925	1758	20540	12690	12376	23828	12344
20	239475	269534	20967	20652	13799	8558	13132	16020
Časové okno	S5 VP	S5 MP	S6 VP	S6 MP	S7 VP	S7 MP	S8 VP	S8 MP
1	12564	35470	13961	169992	15627	13709	198	34574
2	14953	15514	13072	127925	8737	11027	8072	22815
3	14364	1174	12891	93973	4514	36025	655	39117
4	10758	13274	74505	12101	22872	17842	7962	10588
5	22321	3665	10349	100791	20283	42657	16311	14729
6	16482	9610	10664	107373	15756	4158	5293	11143
7	17157	3600	10468	12289	15310	53338	19572	2912
8	13744	4559	107892	15150	29546	19553	3229	6660
9	12626	11320	13048	100321	22602	45014	5179	1946
10	8878	16217	42194	49306	34976	15409	160	9377
11	12591	23938	129798	43836	20951	13799	28919	1686
12	12477	1873	33289	121329	19977	33510	17135	3663
13	126363	9092	32022	17651	21829	7591	14280	15836
14	8540	35116	24770	37576	19983	12234	14674	14796
15	19421	7514	23485	16133	190179	41651	9077	16458
16	23946	2106	19234	21346	12094	8195	14697	7820
17	18615	5741	33706	37033	10918	8664	18049	1454
18	13734	1916	21634	15021	21668	20060	16140	4676
19	12255	19214	34659	69526	51112	15784	29993	5124
20	17357	5919	23609	29141	14042	16394	12928	11226

Tabulka 33: Tabulka počtu hran v temporálních sítích

Časové okno	S9 VP	S9 MP	S10 VP	S10 MP
1	90782	11857	31908	28805
2	19167	14881	24867	9818
3	15599	13248	82176	31377
4	18438	13895	24658	33802
5	17256	17298	22655	29738
6	18469	10384	73698	32116
7	20897	15906	43479	15063
8	18305	16219	18654	10131
9	12557	18569	17917	8602
10	14447	9588	82870	15847
11	23063	10715	30810	35287
12	18512	17238	38463	8622
13	15278	18194	31120	16567
14	14400	15112	42480	22470
15	17907	2425	47187	24595
16	22588	16344	13039	14660
17	25234	13532	5654	5732
18	17429	13882	50827	22922
19	18144	10035	31291	40365
20	17357	16823	66777	9098

Tabulka 34: Pokračování tabulky počtu hran v temporálních sítích

Časové okno	S1 VP	S1 MP	S2 VP	S2 MP	S3 VP	S3 MP	S4 VP	S4 MP
1	2,902	3,569	8,812	3,997	3,013	2,733	3,124	3,131
2	2,552	7,403	3,406	3,554	3,793	3,547	7,413	3,072
3	3,155	3,944	3,663	3,134	2,229	3,347	3,539	3,091
4	3,181	7,412	2,857	2,846	2,231	4,521	4,074	9,569
5	2,671	3,786	3,513	3,395	3,158	3,235	3,268	4,137
6	4,521	3,807	3,313	3,283	11,990	4,456	56,462	3,050
7	2,656	5,893	3,939	3,428	3,357	17,477	3,992	3,558
8	4,59	3,030	2,808	3,736	2,932	3,154	4,458	3,041
9	3,370	2,975	2,928	2,439	3,623	2,864	4,889	3,049
10	7,021	2,861	3,685	2,646	3,190	3,459	3,241	7,950
11	3,979	4,074	2,458	3,573	3,682	3,006	6,072	4,160
12	3,163	10,620	10,487	3,520	3,029	4,348	6,117	2,699
13	10,335	69,670	3,525	3,327	3,482	3,250	5,346	3,427
14	6,677	26,320	3,492	2,633	5,642	4,557	5,147	3,720
15	29,510	73,900	5,217	3,553	3,202	3,611	3,741	2,799
16	19,500	26,610	6,189	4,557	3,115	2,967	4,543	4,43
17	75,790	37,710	3,175	2,929	2,959	2,689	3,438	3,815
18	105,900	13,120	3,007	2,956	3,600	5,360	4,070	3,388
19	75,470	33,930	2,542	3,787	2,872	2,852	5,784	4,846
20	41,320	52,290	3,420	3,594	2,843	2,811	4,057	3,250
Časové okno	S5 VP	S5 MP	S6 VP	S6 MP	S7 VP	S7 MP	S8 VP	S8 MP
1	3,485	10,740	3,017	40,14	3,680	3,547	1,859	8,064
2	2,861	3,018	2,897	32,940	3,105	3,146	3,239	5,530
3	3,132	5,448	2,738	21,750	4,646	7,757	2,584	10,266
4	3,665	3,872	16,880	3,181	4,793	4,526	5,301	3,585
5	3,973	2,788	2,907	16,830	4,077	12,110	5,909	3,659
6	3,811	3,266	3,059	18,940	3,116	3,305	12,140	3,745
7	4,134	4,645	2,905	3,290	3,211	15,120	12,090	2,946
8	3,069	2,521	30,310	2,716	6,401	4,522	2,921	3,723
9	2,693	3,399	3,136	18,070	4,043	8,922	3,853	3,484
10	2,755	2,793	9,041	10,650	6,915	4,448	1,798	4,083
11	2,688	11,093	43,410	8,149	4,947	3,931	5,652	6,333
12	2,578	2,499	7,377	24,490	4,226	7,930	3,612	4,742
13	26,390	4,032	7,391	3,529	4,757	3,164	3,598	3,516
14	4,393	6,351	3,986	6,613	4,127	3,032	3,475	3,667
15	3,708	3,034	4,836	3,442	47,060	9,811	3,006	3,483
16	4,272	3,172	3,935	3,751	2,806	2,975	3,121	3,808
17	3,813	3,423	5,848	6,712	3,216	3,185	3,742	2,101
18	2,851	3,003	5,826	3,046	5,336	6,137	3,749	3,028
19	2,733	2,581	7,661	15,190	11,780	3,417	9,383	2,895
20	4,206	2,799	3,759	6,038	3,477	3,465	3,355	4,227

Tabulka 35: Tabulka průměrných stupňů v temporálních sítích



Časové okno	S9 VP	S9 MP	S10 VP	S10 MP
1	17,220	2,590	7,207	6,583
2	4,120	2,827	3,774	3,061
3	2,899	2,630	15,55	4,181
4	3,758	2,637	5,352	9,512
5	3,327	4,110	4,123	6,596
6	3,611	3,060	13,680	6,518
7	4,112	3,082	10,430	4,150
8	3,546	2,972	3,834	2,625
9	2,769	3,545	3,417	3,004
10	2,807	2,502	16,600	2,894
11	4,230	2,908	6,815	8,937
12	3,587	3,560	6,965	2,717
13	3,147	3,762	5,855	13,360
14	3,148	2,871	8,488	4,202
15	3,510	3,742	9,099	5,054
16	4,122	2,978	3,692	4,845
17	4,820	2,651	2,893	3,476
18	3,455	3,383	9,863	4,112
19	3,330	2,942	5,402	8,917
20	3,376	3,135	12,750	3,167

Tabulka 36: Pokračování tabulky průměrných stupňů v temporálních sítích